

AD-A149 829

CLASSIFICATION MANAGEMENT

DTIC FILE COPY

C

M

JOURNAL of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XX - 1984

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT Unclassified/Unlimited		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION National Classification Management Society		6b. OFFICE SYMBOL (If applicable)		7a. NAME OF MONITORING ORGANIZATION	
6c. ADDRESS (City, State and ZIP Code) Executive Secretary NCMS 6116 Roseland Drive Rockville, MD 20852				7b. ADDRESS (City, State and ZIP Code)	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State and ZIP Code)				10. SOURCE OF FUNDING NOS.	
				PROGRAM ELEMENT NO.	
				PROJECT NO.	
				TASK NO.	
				WORK UNIT NO.	
11. TITLE (Include Security Classification) Journal of the National Classification Management Society (over)					
12. PERSONAL AUTHOR(S) Eugene Suto and DeLoris Goldsby					
13a. TYPE OF REPORT		13b. TIME COVERED FROM _____ TO _____		14. DATE OF REPORT (Yr., Mo., Day) 1984	
15. PAGE COUNT					
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB. GR.			
19. ABSTRACT (Continue on reverse if necessary and identify by block number)					
DTIC ELECTE S JAN 28 1985 A					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS <input type="checkbox"/>			21. ABSTRACT SECURITY CLASSIFICATION		
22a. NAME OF RESPONSIBLE INDIVIDUAL Eugene Suto			22b. TELEPHONE NUMBER (Include Area Code) 893-5900		22c. OFFICE SYMBOL

11. Volume XX - 1984

2

CLASSIFICATION MANAGEMENT

DTIC
ELECTE
S JAN 28 1985 D
A

**JOURNAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME XX 1984**

This document is to be controlled
in accordance with the policy of
the National Classification Management Society

ISSN-0009-8434

Accession For
 GRA&I
 TAB
 announced
 information

1967
 1968
 1969
 1970
 1971
 1972
 1973
 1974
 1975
 1976
 1977
 1978
 1979
 1980
 1981
 1982
 1983
 1984
 1985
 1986
 1987
 1988
 1989
 1990
 1991
 1992
 1993
 1994
 1995
 1996
 1997
 1998
 1999
 2000
 2001
 2002
 2003
 2004
 2005
 2006
 2007
 2008
 2009
 2010
 2011
 2012
 2013
 2014
 2015
 2016
 2017
 2018
 2019
 2020
 2021
 2022
 2023
 2024
 2025
 2026
 2027
 2028
 2029
 2030
 2031
 2032
 2033
 2034
 2035
 2036
 2037
 2038
 2039
 2040
 2041
 2042
 2043
 2044
 2045
 2046
 2047
 2048
 2049
 2050
 2051
 2052
 2053
 2054
 2055
 2056
 2057
 2058
 2059
 2060
 2061
 2062
 2063
 2064
 2065
 2066
 2067
 2068
 2069
 2070
 2071
 2072
 2073
 2074
 2075
 2076
 2077
 2078
 2079
 2080
 2081
 2082
 2083
 2084
 2085
 2086
 2087
 2088
 2089
 2090
 2091
 2092
 2093
 2094
 2095
 2096
 2097
 2098
 2099
 2100
 2101
 2102
 2103
 2104
 2105
 2106
 2107
 2108
 2109
 2110
 2111
 2112
 2113
 2114
 2115
 2116
 2117
 2118
 2119
 2120
 2121
 2122
 2123
 2124
 2125
 2126
 2127
 2128
 2129
 2130
 2131
 2132
 2133
 2134
 2135
 2136
 2137
 2138
 2139
 2140
 2141
 2142
 2143
 2144
 2145
 2146
 2147
 2148
 2149
 2150
 2151
 2152
 2153
 2154
 2155
 2156
 2157
 2158
 2159
 2160
 2161
 2162
 2163
 2164
 2165
 2166
 2167
 2168
 2169
 2170
 2171
 2172
 2173
 2174
 2175
 2176
 2177
 2178
 2179
 2180
 2181
 2182
 2183
 2184
 2185
 2186
 2187
 2188
 2189
 2190
 2191
 2192
 2193
 2194
 2195
 2196
 2197
 2198
 2199
 2200
 2201
 2202
 2203
 2204
 2205
 2206
 2207
 2208
 2209
 2210
 2211
 2212
 2213
 2214
 2215
 2216
 2217
 2218
 2219
 2220
 2221
 2222
 2223
 2224
 2225
 2226
 2227
 2228
 2229
 2230
 2231
 2232
 2233
 2234
 2235
 2236
 2237
 2238
 2239
 2240
 2241
 2242
 2243
 2244
 2245
 2246
 2247
 2248
 2249
 2250
 2251
 2252
 2253
 2254
 2255
 2256
 2257
 2258
 2259
 2260
 2261
 2262
 2263
 2264
 2265
 2266
 2267
 2268
 2269
 2270
 2271
 2272
 2273
 2274
 2275
 2276
 2277
 2278
 2279
 2280
 2281
 2282
 2283
 2284
 2285
 2286
 2287
 2288
 2289
 2290
 2291
 2292
 2293
 2294
 2295
 2296
 2297
 2298
 2299
 2300
 2301
 2302
 2303
 2304
 2305
 2306
 2307
 2308
 2309
 2310
 2311
 2312
 2313
 2314
 2315
 2316
 2317
 2318
 2319
 2320
 2321
 2322
 2323
 2324
 2325
 2326
 2327
 2328
 2329
 2330
 2331
 2332
 2333
 2334
 2335
 2336
 2337
 2338
 2339
 2340
 2341
 2342
 2343
 2344
 2345
 2346
 2347
 2348
 2349
 2350
 2351
 2352
 2353
 2354
 2355
 2356
 2357
 2358
 2359
 2360
 2361
 2362
 2363
 2364
 2365
 2366
 2367
 2368
 2369
 2370
 2371
 2372
 2373
 2374
 2375
 2376
 2377
 2378
 2379
 2380
 2381
 2382
 2383
 2384
 2385
 2386
 2387
 2388
 2389
 2390
 2391
 2392
 2393
 2394
 2395
 2396
 2397
 2398
 2399
 2400
 2401
 2402
 2403
 2404
 2405
 2406
 2407
 2408
 2409
 2410
 2411
 2412
 2413
 2414
 2415
 2416
 2417
 241

Published by the National Classification Management Society. Mailing Address: Executive Secretary, NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editors of this volume: Eugene Suto and DeLoris Goldsby. The information contained in this Journal and presented by the several individuals does not necessarily represent the views of the organizations they represent — unless they are the head of the organization—nor of the National Classification Management Society.

Copyright © 1984 National Classification Management Society

TABLE OF CONTENTS:

Proceedings of the Twentieth Annual Seminar (Technology Transfer—A National Security Problem)—

PART I—Speakers

FOREWORD	v
President Ronald Reagan's Letter	
KEYNOTE	1
Maynard C. Anderson	
DEFENSIVE INVESTIGATIVE SERVICE—CURRENT ISSUES ;.....	6
Thomas C. O'Brien	
U.S. STATE DEPARTMENT APPROACH TO TECHNOLOGY TRANSFER ;.....	22
Allan E. Suchinsky	
ENFORCEMENT OF CRIMINAL LAW RELATIVE TO STRATEGIC EXPORTS ;.....	27
Joseph J. Tafe	
OPSEC FROM THE STANDPOINT OF AN IMPLEMENTER ;.....	34
Thomas J. Conner	
GOVERNMENT SECURITY REQUIREMENTS—A THOUSAND FACES TO INDUSTRY ;...	38
Irving T. Boker	
SECURITY RESPONSIBILITIES FOR MANAGERS ;.....	43
James Mood	
TECHNOLOGY TRANSFER DEVELOPMENTS AT THE OSD LEVEL ;.....	48
Anthony G. Mitchell	
David Whitman	
FOREIGN OWNERSHIP, CONTROL AND INFLUENCE (FOCI) ;.....	54
James J. Bagley	
G. Christopher Griner	
TECHNOLOGY TRANSFER ;.....	63
James W. Dearlove	
TECHNOLOGY TRANSFER—A BRITISH PERSPECTIVE ;.....	86
John S. McMichael	
TECHNOLOGY TRANSFER—A CANADIAN PERSPECTIVE ;.....	90
Robert T. Grogan	

COMPUTER ABUSE AND THE HACKER ;	96
David C. Brown	
DoE INITIATIVES IN TECHNOLOGY TRANSFER ; <i>and</i>	99
Robert R. Freclund	
PROTECTING ADVANCE CONCEPTS AND TECHNOLOGY ;	109
Joseph R. Cacek, Jr.	
DoD/INDUSTRY PANEL	111
Gerald L. Berkin	
Joseph F. Murray	
John McMann/David Whitman	
Dean Richardson	

PART II—Workshops

1. CLASSIFIED DOCUMENT MARKING ;	123
Sheila K. Daigle	
2. HOW TO PREPARE A MATRIX SECURITY, CLASSIFICATION GUIDE ;	133
Herman H. Teifield	
3. PREPARATION OF DD FORM 254 ;	136
Andrea Wraalstad	
4. DEPARTMENT OF ENERGY WORKSHOPS ;	148
Maria Barela, George Carnahan, Charles Demos	
5. DERIVATIVE CLASSIFICATION IN ACCORDANCE WITH A SECURITY CLASSIFICATION GUIDE ;	162
Joseph A. Grau	
6. INTELLIGENCE MARKINGS ; <i>and</i>	168
Ron Weaver, David Whitman	
7. CLASSIFICATION MARKINGS ;	172
Sheila K. Daigle, Elaine Gruber	
Set 1. Classification Pending	
Set 2. Special Access Markings	
Set 3. Classifying Authority and Downgrading/Declassification	
Set 4. Remarking Classified Material Originated Prior to August 1982/Compilations/ Working Papers	
Set 5. Classification Markings/Symbols	
Set 6. Document Marking Practical Exercise.	

PART III—Annual Report and Awards 187

PART IV—Charter Members Program and Seminar Photos 191

PART I

Proceedings of the Twentieth Annual Seminar

Speakers

22–25 May 1984

**Showboat
Las Vegas, Nevada**

FOREWORD

**The White House
Washington
May 17, 1984**

I welcome the opportunity to extend my best wishes to officers and members of the National Classification Management Society as you gather for the Society's twentieth anniversary.

Since its inception in 1964, the Society, through its efforts to promote professionalism in the information and industrial security fields, has done a great deal to improve the security posture of our Nation. Its security education and training programs bridge the gap between government and industry and foster that spirit of cooperation so necessary to the successful accomplishment of our national security objectives.

Moreover, the Society has played a significant role in the development of Executive Orders and departmental regulations which have governed the information security program, including Executive Order 12356, National Security Information. The annual report of the Information Security Oversight Office covering the first year under the new Order has shown that we have improved significantly the credibility and efficiency of the classification program. Our success is due in no small part to the efforts of the fine professionals of the NCMS.

The theme of the Society's Twentieth Anniversary Training Seminar, "Technology Transfer," is of particular interest at this time because of the serious threat the loss of our sensitive technology poses to our security.

I know the Society will keep up its fine work and wish all of you continued success in the coming years.

/s/ Ronald Reagan

KEYNOTE

Maynard C. Anderson
Director
Security Plans and Programs
Office of the Secretary of Defense
Washington, D.C.

Greetings and best wishes for a successful 1984 training seminar on the twentieth anniversary of your organization. George Bernard Shaw is reported to have written, "For every complex problem, there is a simple solution—and it is always wrong." That is an apt warning that should give us a premonition, at least, to treat this business of technology transfer with the respect that it deserves.

To begin any discussion of your theme, I would suppose we should agree to accept the definition of "technology" that has become official within the Department of Defense, at least, with the publication of a directive concerning the matter. Technology is "the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves."

This definition encompasses ideas, innovation, creativity, all significant to the maintenance of the informational advantage of the West in the world community. Protection of that informational advantage becomes a goal within the United States objective of *controlling* technology transfer, while maintaining the competitive position of American Industry in the world market.

The definition of technology does not restrict us to the consideration of either classified or unclassified information. Our traditional, structured approach to the control of classified information, however, eliminates that category of material from principal concern when we discuss technology transfer.

Since we know that our classification systems works, sometimes too well, it would seem that we might take some lessons from our background of knowledge and experience in the information classification system and apply them to the control of technology.

It is in this regard that the National Classification Management Society has much to offer in bringing to bear on this issue the extraordinary assets of its membership. As you provide for exchanges of views concerning information security programs, it was inevitable that you would come to the decision to examine the issue of technology transfer because it involves information, the indiscriminate disclosure of which is damaging to the national interest both in terms of military systems and economic welfare.

I am delighted to be able to discuss some aspects of the matter with you this morning because you have been in the forefront of past efforts to ensure that the government's philosophies for protecting information in the interest of the national defense have been understood. You can help us now in promoting understanding of the dimensions of problems involved in dealing with this different kind of information.

There is no other single issue that surpasses technology transfer in the ability to cause intense debate among representatives of government, industry, the scientific, academic and technical communities today. That pleases me because out of such constructive conflict comes many innovative ideas.

In the context of conflict, however, we might recall an admonition from Proverbs Chapter 25, 9th verse, "Argue your case with your neighbor, and do not reveal the secret of another."

We all have equities in this issue, some stronger than others, but I would submit that by consideration of all concerns, we will emerge with a stronger national base. I hope that you and I can begin today to reach some measure of agreement that will strengthen our sense of mutual responsibility in dealing with this subject and its issues. It has been established that technology transfer is a multifaceted creature involving research and development, communications, international trade, political and economic policy, with implications in the realm of security.

There are, consequently, some competing interests. For example, the United States Government encourages exports to promote employment and an improved balance of payments. At the same time, the United States Government

does not want to let go of something that would weaken our national defenses if in Soviet hands.

In a message to the Congress on 11 July 1983, President Reagan stated, "We are continuing our cooperation with the U.S.S.R. in science and technology. This is a complex matter made more difficult because of Soviet behavior regarding Afghanistan and Poland, as well as their efforts to acquire sensitive Western technology. Decisions to renew agreements are being made on a case-by-case basis taking these concerns into account along with the benefits to the U.S. through participation. For example, I have recently approved the renewal of an agreement for cooperation with the Soviets on atomic energy, with appropriate limitations to protect our interests while letting the work proceed."

The United States is not going to abandon free trade. But, our policies are intended to make it more difficult for our adversaries to acquire some of the sophisticated technology they need to match Western weapons. We would hope to balance protection with profits.

It has been written that "Technology is the natural foe of Nationalism", and "there is a sense of cooperative accomplishment among the 'Republic of Technologists', regardless of national loyalties." This is another aspect of the problem that, unfortunately, sometimes affects both classified and unclassified information as we struggle with the problem of mitigating damage done by "cross talk."

It is clear that the objectives of the Soviet Union are inimical to our own in the areas of military and dual use technology. There is much evidence available to prove the intensity and size of the effort by the Soviet Union to collect Western technology. It is not surprising when you think about Soviet goals:

- To maintain parity, if not superiority, the Soviets recognize readily that the real test may be not who first develops technology, but rather, who is first to use it effectively;
- To save money on research and development by acquiring proven technology;
- To save research time;
- To speed production of weapon systems;
- To rapidly develop countermeasures;

- To avoid costly and time consuming mistakes; and
- To know in advance that a system will work.

The "vacuum cleaner" approach used by the Soviet Union and its surrogates to collect Western information must result in a great hall filled with analysts who attempt to determine the relative worth of all that comes to them. Those analysts and the politburo bosses obviously subscribe to the old Hebrew proverb, "Quality is more important than quantity; but is best in large numbers."

The theft of information from the West has become therapy that somewhat relieves the Soviets of their often paranoic feelings toward the west, perhaps, and, as Dr. Fred Ikle, the Under Secretary of Defense for Policy, has speculated, we might well be creating a group of lazy soviet scientists. These salutary benefits in addition to creating a Soviet dependence which could always keep them a couple of years behind, are not enough, unfortunately, to justify our failure to restrict from their acquisition information of significance to our national defense.

How should we attack this problem? In recognition of the fact that we have been, and perhaps are now being taken advantage of, how do we balance the necessity for protection, with the necessity for free trade, with the rights of academics and researchers, not to mention the rights of individuals, in finding a reasonable solution?

Henri Regnard, a distinguished French civil servant, writing in *Defense Nationale*, December 1983, established a broad premise for future action after he described Soviet collection efforts: "This range of hostile activities calls for the closest kind of collaboration at European and Western levels. It requires the development of a whole complex of new defensive measures aimed at enclosing east-west exchanges, particularly those in the trade, scientific, and technological areas, in a more selective, if not more restrictive framework."

Prime Minister Thatcher, addressing the Parliament in a prelude to submission of the report of the Security Commission concerning the prime case last year, stated her government's case for security with great eloquence: "All security procedures imply some degree of encroachment upon the rights and freedoms of the individual. We

have to decide how to strike the balance between those considerations and the need to protect national security, in laying down security procedures that will be as effective as possible within the limits of what is acceptable in a free and democratic society. In doing so, we have to bear in mind that no system of security can be guaranteed to confer absolute protection; even in a totalitarian society, it is not possible to be sure that there are no spies."

The Soviet Union, while stealing our technology, has not overlooked the fact that whatever they have developed that is worth lifting must be protected. The Soviets are treating the problem in typical fashion. On 3 February 1984, the New York Times reported that "The Soviet Union has promulgated a new law providing prison terms for anyone passing economic, scientific, technical or other 'official' secrets to foreigners. Passing and gathering with the intention of passing to foreign organizations or their representatives economic, scientific-technological or other information comprising official secrets, by a person to whom this information was entrusted through service or work or became known by other means, will be punished by deprivation of freedom for up to three years or corrective work for up to two years."

The principal commodity with which you deal is information and I would submit that it is our greatest concern. Export controls and trade policies are not enough to control the loss of the technology edge. They will not, for example, affect the loss of technology right here through technical and professional publications, or through the purchase of commercially available end products.

David S. Brown, Professor of Management, George Washington University, has written that "The gifted thief steals ideas, not things." That puts our concern today into proper perspective. He has also written that, "The greatest contribution to openness of governmental administration is not the Freedom of Information Act, but the xerox." That may be true, and the xerox may be a contributor of significance to uncontrolled technology transfer as well.

William B. Bader, Vice President SRI-International, Washington, has speculated that our task

may be larger than we believe: "In the long run, it may be impossible for a country like the United States to limit the flow of technology and knowledge, even if it wants to. The United States has thrown open its universities, research laboratories and corporations to citizens from abroad. About 300,000 foreign students, eight times as many as in 1954, are enrolled in United States colleges and universities."

Somewhat in support of the extraordinary dimensions of the problem is the opinion of Stephanie G. Neuman, International Organization, Winter 1984, that technology has replaced military end-items as the new medium of exchange in the world's arms trade.

Despite the size and complexity of the problem we have elected to consider, it must be treated. I would think that we should begin the ministrations by establishing that creativity and innovation in findings solutions are required.

If we establish the environments that are receptive to the results of creative thinking, innovative solutions will follow which will influence our established institutions to take appropriate actions. "Most organizations today cannot be controlled. Today's institutions can be influenced and managed, but they are not responsive to any unilateral decree or decision." (David S. Bushnell, George Mason University, and David H. Bennet, Dynamic Systems, Inc., "Management is an unnatural act," The Bureaucrat, Spring 1984.)

Creative solutions will provide necessary institutional influence. Security planning, to include planning for the control of technology, must follow national planning. Dr. Ikle's writing in Strategic Review, Fall 1983, stated "It is also important that we exploit every means of encouraging the Soviets to slow down their military build up over the longer run, thus dampening the arms competition and enabling the United States to spend a greater share of its resources for much-needed domestic purposes. This objective accounts for the emphasis the Reagan administration has placed on controlling the transfer of technology to the Soviet Union. It is axiomatic that the greater the flow of militarily relevant Western technology into the Soviet military-industrial base, the easier it becomes for the Soviet leadership to sustain and even accelerate the current momentum of Soviet military programs."

"Another way of making it easier for us to compete with the Soviet Union in the long term is to pursue technological advances that will have the effect of hastening the obsolescence of Soviet equipment. The accumulated assets in Soviet arsenals cannot be matched by the west, tank for tank and missile for missile. Even trying to do so would entail substantially enlarged U.S. and allied defense budgets and efforts. Yet, we do have it in our power to harness technology and tactical innovations in order to bring about an accelerated depreciation of those Soviet assets."

The protective systems we devise then must be responsive to national priorities, economically feasible, and flexible. To begin with, you and I must determine what information needs protection. Because of the burgeoning availability of information, the dynamics of maintaining an informational advantage will mean more resources must be devoted to discriminating among sensitivities of information in order to be able to protect that which is truly sensitive, and, that includes information that is not otherwise available to an adversary.

I believe the concept of classification management will be translated into reality by modern technological means—not because program managers will want it any more, but because they will have no choice. And, finally, because we have the tools to make it work. Resources will not keep up with the requirements that exist today, let alone what are forecast for tomorrow if program managers continue to seek protective shrouding for their information at the same pace as they do today, so protection priorities must afford coverage to only that which is essential, and they must be dynamic in order to keep up with changing environments, obsolescence and foreign availability of technology.

Information control procedures must be determined on the basis of strategic treatment and deal in broad principles, circumstances, threats, environments and vulnerabilities differ and will differ more and more rapidly as change becomes more rapid. Your creativity will be tested as you apply the proper protective techniques in response to the particular challenges you face in any given set of circumstances.

Willis H. Ware, "Information Technology Crime and the Law," The Rand Corporation, November

1982, says, "Keep your eye on the functional role of the information system, for therein will be the crime. Do not be misled by the manner in which information is represented—on magnetic tape, on cards, on paper, on video discs. Moreover, do not be confused by how it is manipulated—by computer, by computer and communications, by manual methods, or a combination of them. Furthermore, do not be misled by the way information is transported—by satellite, by microwave, by pony express, or by U.S. Mail. Keep your eye on the information, how it is used, misused or laundered; and, how it relates to the crime or the abuse to be deterred. Target the law accordingly."

During the recent past, we have embarked on a course of information management which concentrates on emphasizing and extending the regulatory process over critical military technology. Mr. Anthony Mitchell, my Deputy for Information Security and Mr. David Whitman of his staff will discuss facets of this, and others will acquaint you with other aspects of the U.S., Canadian and British programs. Since you will hear much discussion of the details of those processes over the next few days, let me leave them with merely a mention, and take a slightly more esoteric path.

We have given little consideration to the human factor involved in this problem. Contrary to our concerns for personnel security in the realm of dealing with classified information, we have done nothing to ensure that the technology embargoed from export, or otherwise identified as critical to the national security, is in the hands of trustworthy people.

One must ask whether it is logical to take all of the regulatory steps to protect sensitive, national security related technology while disregarding a need for some determination of the integrity or the motivations of the custodians of that information? Penalties for illegal export will not reach the extent of persuasion required. Therefore, I would suggest that once reasoned decisions have been made as to what must be protected, some means must be devised to ensure its custodian's responsibility.

The preferable mean, of course, is a relationship between custodian and employer, whether government or industrial, which fosters alle-

giance through loyal participation in the enterprise to include sharing of burdens and profit, and, which would make betrayal of trust repugnant despite the ideological or economic temptation.

Another means would be an administrative process (quasi-judicial) under which individual failures to accept the responsibility for protection are subject to penalty. What I am suggesting, of course, is a covenant between the government and the individual, just as we must have between the government and an industrial enterprise, a mutually binding contractual agreement. I don't mean to be a skeptic by insisting that our information custodians be legally bound, but the necessity for oath taking in legal proceedings does not speak well for the probity of witnesses, and perhaps we can learn a lesson from that.

In the now famous *Snepp* decision, all members of the court agreed that even in the absence of a written contract, under the common law, an employee has a fiduciary obligation to protect confidential information obtained during his employment and that a breach of this obligation could be punished by the seizure of personal profits from the exploitation of such information. Perhaps this principle is worth considering in determining means by which a custodian of designated technology may be obligated to its protection and punished for failure to adhere to such an obligation.

In the fourth century before Christ, Demosthenes wrote: "There is one safeguard known generally to the wise, which is an advantage and security to all, but especially to democracies as against despots. What is it? Distrust."

In order to reconcile our security policies with the place of technology in the world, there is needed a clear understanding that there must be some parity between the two. There must be a recognition that there is mutual benefit from cooperative management in which a security sys-

tem has been created that allows both the development and exploitation of technology to take place. There must be an admission that the national interest is served sometimes by sharing technology, both among ourselves and with others in the world. There must be an acceptance of the fact that suggested guidelines for security often inspire better judgment and more creative application through the conferring of responsibility than does the imposition of hard, inflexible rules within which there is no opportunity for participants in the program to exercise good old American initiative and resourcefulness.

We cannot adjust events to policies. We must be ready to respond to the uncertainties that we will surely face. During these few minutes, I have mentioned creativity and innovation more than once as assets which we must employ in meeting the new and uncertain challenges in maintaining control over technology transfer. I am of the happy faith that you will bring to bear on this issue the twenty years of accomplishments and achievements that are represented here this morning. And it is necessary that you do just that because I believe as the editorialist in the *Philadelphia Inquirer* wrote on September 25, 1981, that "Individual institutionalized liberty lies at the heart and the minds of the immensely complex competition between the United States and its allies on one hand and the forces of tyrannical repression on the other," but "the price of liberty is not to strangle it."

And, a personal note. I have known many of you here for many years. I know of your efforts, both privately and collectively that have been dedicated to the preservation of our national security. I would say to you, in closing, some words that I wrote to a former leader of this organization, Frank Larsen: "When I cannot help but place myself in the position of George Santayana's thoughtful man who might ask whether the present civilization is the last one the world will see, I can answer that if it is, you will be among those who helped make it the best the world has ever seen."

THE DEFENSE INVESTIGATIVE SERVICE
*An Active Partner in the Government's Effort to
 Control the Export of Technology*

Thomas J. O'Brien
Director
Defense Investigative Service
Washington, D.C.

Recently I was asked, "What do the Departments of State, Commerce, Defense and Energy and the Nuclear Regulatory Commission (NRC), Customs, Federal Bureau of Investigation (FBI) and the Defense Investigative Service (DIS) all have in common?" I thought for a minute and said, "I don't know." The questioner then advised me that we all have a role in securing America's high technology. The contractor then asked me, "Who is in charge of this effort?" And, again, I said, "I don't know." The questioner then said, "I don't either." The commentary, in a sense, sums up a part of the problem. There are many agencies involved in this very complex and difficult area, but we don't really have a "team captain." This factor, in itself, makes the problem difficult to deal with but I submit to you that this organizational aspect is only part of the problem.

What are some of the others? First, we all recognize that the administration of any security or control system in a free society is a very difficult task. This is one area where we cannot and, indeed, should not be competitive with the Soviet Union. In our open society and democratic way of life, security control systems run against the grain! Inherently, there will be difficulties and problems.

Another part of the problem is the fact that technology in the United States and, indeed, throughout the Free World, is a very lucrative target. The Soviets and their partners in the Warsaw Pact have long recognized the value of the Free World's technical exploits and they have mounted a very sophisticated and well-financed effort to obtain this technology. They recognize, and we should recognize, that much of their success in building up their defense establishment is due to the technology which they have been able to obtain from the West.

The dimensions of the problem do not stop here. The first really effective export control legislation which led to the establishment of a listing

of munitions and implements of war was the Munitions Control Act. It came about in the 1930's as a follow on to military rearming after World War I. The first Export Control Act was enacted in 1949, shortly after World War II. Both the International Traffic in Arms Regulations (ITAR) which implement the Munitions Control Act and the Export Administration Regulations, which pertain to the Export Control Act, were developed during periods of history when the primary focus of attention was on implements of war, commodities, products and hardware. These were the primary considerations. Almost as an afterthought, the ITAR states "and also information relating thereto." I submit to you that one of our problems is that our concept and approach to dealing with export control was designed during the period of time when export of products was the main focus of attention. Today, during this period of "the information revolution," high technology-information critical to weapons design is as important if not more important than the hardware itself. My question is, "Has the legislative and regulatory approach kept pace with the shift from commodities and implements of war to the information which embodies today's high technology?"

Traversing all of these problems is the fundamental competing considerations of free trade versus restrictions which are intertwined with the whole area of export control. One of the major problems facing the United States today is the trade deficit and the unfavorable balance of payments which is now approximately 70 billion dollars. The U.S. economy depends upon an environment conducive to free trade. Control of exports seriously inhibits the open market which is so essential to the long term economic well being of the United States and the rest of the Free World.

So much for the big picture and the big problems. What are some of the solutions and how does the Defense Industrial Security Program fit into the picture? First, I want to point out that our Industrial Security Program is preventively oriented vice punitively oriented. In the U.S. society, voluntary compliance by its citizens, including its corporate citizens, is our greatest strength and greatest asset. It is in this area of voluntary compliance that the Defense Industrial Security Program plays its primary role. *I submit to you that we are losing more technology today because of a lack of awareness and a lack of understanding*

rather than because of calculated and pre-meditated efforts to circumvent export controls. Our job in this area is to increase the level of awareness and level of understanding. DIS has a unique relationship with over 12,700 cleared facilities throughout the United States which employ approximately 1.4 million cleared personnel. These facilities and their employees are on the cutting edge of today's technology. By increasing awareness and understanding of the rules governing export of technology, we will take a significant step forward in promoting the voluntary compliance that is so essential to successfully combat the current technology drain.

Now, let me be a little more specific. For many years, the Industrial Security Manual has directed specific attention to the requirements of the ITAR and the Export Administration Regulations. Therefore, a contractor by virtue of his involvement in classified procurement, will be reminded of his related responsibilities in the area of technology export.

In addition, the Industrial Security Manual provides a very structured system for the identification and safeguarding of classified information. We feel controls work well and as a result export of classified information is denied, except where specific information is authorized to be shared with selected allies on a government-to-government basis.

The Industrial Security Manual also establishes the specific requirements governing unclassified information related to classified contracts. A contractor may not publicly disclose nor export unclassified information in this category without specific approval from the Department of Defense. This provision is particularly significant in marketing endeavor and in the control of technology released at meetings and international symposiums.

In another area, the Industrial Security Manual establishes very definitive requirements for providing defensive security briefings to people who travel to Communist countries or who attend international conferences or symposiums where representatives from Communist countries will be in attendance. By alerting these people to the potential dangers that these types of international meetings might generate, we reduce the

likelihood of inadvertent or unintended disclosures.

We also have a system whereby contractors must report unclassified visits to their U.S. facilities by representatives from Communist countries. By requiring such visits to be reported, and by reminding contractors of their responsibilities to brief and alert all of their personnel who will be hosting or briefing the foreign visitors of the information disclosure prohibitions, including the ITAR and the Export Administration Regulations prohibition, we reduce the likelihood that representatives from Communist countries will gain access to embargoed technologies.

Today, there are approximately 6,500 cleared employees of U.S. contractors permanently stationed abroad. In addition, some 10,000 cleared employees of U.S. contractors make annual foreign visits. The Industrial Security Program directs special attention to these personnel. We require that procedures be established to indoctrinate these personnel with a view toward ensuring that they are well versed on security requirements. Specifically, that they know what is and what is not authorized for public release and foreign disclosure.

In the Industrial Security Program, we also look to each cleared facility to determine whether or not it is under foreign ownership or influence. As a part of this process, we require the contractor to disclose the existence of contracts, licensing agreements, patent arrangements and trade secret agreements with foreign interests. This gives us the opportunity to remind the contractor of the statutory obligation to comply with the International Traffic in Arms Regulation and the Export Administration Regulations. We also assess the possibility that foreign influence might result from interlocking directors from foreign corporations. Our effort in monitoring foreign ownership or control of U.S. companies serves to heighten the level of awareness and reduce the likelihood that this type of foreign entanglement will result in a conduit for the improper or illegal export of technology.

The foregoing is a listing of some of the more specific requirements directed to the heart of the technology export problem. We have, in addition, the general security awareness which results from the inspections of our cleared facilities.

Generally speaking, our Industrial Security Representatives inspect facilities every six months (some are on a 9-month schedule). One of the benefits of these inspections is to promote general security awareness or what we like to call "a security environment."

In addition, we frequently publish articles in the Industrial Security Letter which directs specific attention to issues involving control of technology. We also publish a Security Awareness Bulletin. The issue of February 1983 was devoted exclusively to technology transfer. This publication has been widely acclaimed as "must" reading and an excellent reference for anyone involved in security or responsible for controlling high technology. If you don't have a copy, the Defense Investigative Service will be pleased to make a copy available. We also promote security awareness through the various courses conducted by the Defense Security Institute and through the audio visual products produced by the Institute.

In addition to the foregoing, the Defense Investigative Service cooperates with the FBI in their security or *DECA* briefings for industry. These briefings highlight the threats encountered by industry and directs specific attention to ensure the contractor is aware of and acts in compliance with statutes governing technology export. DIS also cooperates fully with the U.S. Customs Service in their Operation Exodus. Throughout the country, we have provided assistance to Customs' agents in their efforts to intercept illegal exports.

So much for what is being done by the Defense Industrial Security Program. Let me now direct your attention to the most important aspect. What should be done by U.S. industry? It is my suggestion that industry must promote a high sense of awareness. This seminar today, sponsored by NCMS, is a very meaningful step in promoting the kind of awareness that is essential if we, as a Nation, are to be successful in controlling technology exports.

But to get from the general to the specific, I think every company must reassess its approach to this problem. Don't assume that your employees are automatically aware of what information is classified, of what information is related to classified contracts and, therefore, subject to con-

trols. Don't assume that your employees are aware of that body of information covered by the ITAR or the Export Administration Regulation. These are very complex and difficult issues. People are not automatically aware of the parameters. A great deal of attention must be directed to educate, inform and caution.

In addition, each company should be aware of the special problems and pitfalls that confront various categories of their people. I use as an example, marketing personnel. A marketer, to be successful, must be fully knowledgeable of his product and he must employ all the attributes of a good salesman to promote a free exchange of information in order to be successful in his marketing endeavors. Unless specific steps are taken to educate a marketer of the problems and limitations on disclosure, it is almost certain that in a foreign marketing endeavor, he will move beyond permissible parameters.

Similar, although different problems, are faced by your technical and engineering personnel. When an engineer is brought in to solve a technical problem for a foreign client, his natural inclination will be to bring all his technical expertise to bear on the problem. The engineer, unless aware, will not stop to compartmentalize in his mind that information which might be classified or that information subject to export controls. Given the natural training and background of the engineer, his primary focus of attention will be, solving the problem at hand.

A similar problem is encountered by scientific and technical personnel who participate in international scientific meetings and symposiums. Again, their natural inclination will be to "fully" participate. Your role must be, from a security standpoint, to ensure they understand what information may be disclosed and what information must be held back.

Another category of your employees which requires special attention are those who are permanently assigned overseas and those who visit overseas. These people have direct encounters with foreign clients and this poses a particular kind of a risk—a risk that technical data, not authorized for export, will be inadvertently disclosed.

So how does a company go about promoting security awareness? How can companies ensure that their people are attuned to the problem? I suggest that your company establish a *Corporate Technology Control Team* to provide high visibility and oversight to the technology control problem. *This team should be made up of top executives from engineering, marketing, legal and security.* The team's role should be to keep the technology transfer problem front and center to ensure that employees who have occasion to meet with and deal with foreign representatives know what is classified and know what technology is embargoed. Above all, to be successful in this very difficult area, we must have the full support of top management. If top management lets it be known that control of technology and compliance with statutory and regulatory requirements is company policy, we will succeed. Your participation in this conference is a very meaningful step toward a solution to the problem.

Let me talk briefly on our Classification Management (CM) function.

We are continuing to stress our (CM) function in DIS—providing guidance and assistance to contractors and user agencies. Many training sessions have been held over the past year by our classification management (CM) specialists. We now have CM specialists in all regions, with experience in a user agency or a contractor facility, (except the Los Angeles region which is currently vacant). We are placing more emphasis in our review of the guidance provided and are looking for ways and means to improve on our role in this area.

We continue to see many problems with the DD Form 254s which are provided to contractors and subcontractors alike, such as:

1. *The name and address of the contractor subcontractor is not correct.* This is very important since the name and address furnished by the Cognizant Security Office (COG) during the verification process is the address that has been established to receive classified information at the facility. Some facilities have a great volume of registered and certified mail that is normally received by them and establish a specific address solely for the purpose of receipt of their classified mail. If the exact address that is provided by the

Cognizant Security Office (COG) is not used, the possibility of compromise of the classified material is greatly increased.

2. *Guidance is not tailored to the performance of the contract/subcontract.* Entire guides are often cited as guidance on the DD Form 254 when only a small portion of the guide is applicable to the performance of the contract. Extracts or specific reference to certain portions of the guide should be provided. We also see many references to user agency directives, i.e., Air Force regulation No. __, Army regulation No. __, or Navy instruction, etc., should be consulted. These documents are not provided to the contractor and even if they were, normally they would not provide adequate guidance for the performance of the contract. This practice places an unnecessary burden on the contractor and should be avoided.

3. *Item 15 of the DD Form 254 contains only information extracted from the Industrial Security Manual (ISM).* All contractors performing on a classified contract are bound by the security agreement to the provisions of the ISM. Extracts from the ISM do not provide classification guidance to a contractor and often only causes confusion. The ISM provides procedures and guidance for safeguarding classified information that has been provided to the contractor or that has been generated and classified by the contractor using the guidance that was provided with the DD Form 254.

We see many guides and DD Form 254s which are very wordy and look very impressive. However, if the words do not pertain to the performance of the contract and if the DD Form 254 does not provide the contractor or subcontractor with the the guidance needed for his particular contract, it is meaningless.

We solicit your cooperation in trying to improve the guidance and the DD Form 254. With your help and cooperation we can improve this area of the industrial security program. Please feel free to call on our CM specialist in each region if we can be of assistance to you.

Let me now highlight for you some aspects of the DISP workload. Figure 1 shows our growth from FY 1980 where we had 10,869 cleared facilities to FY 1984 where there are currently over 14,000 cleared facilities. (See Figure 1)

There has further been a dramatic increase in contractor facilities with ADP Systems. Please note that these have grown from 994 in FY 1982 to 1588 in FY 1984. (See Figure 2)

Total ADP Systems in use in all these facilities now number over 8,000, providing an ever increasing responsibility upon our ADP Specialists. There is one or more such Specialist assigned in each region. (See Figure 3)

Our DISP contractor inspections have increased to a projected inspection schedule of over 21,000 for FY 1984. (See Figure 4)

With this number of inspections we find the greater majority, 43%, are with no deficiencies. Approximately 3% involve major deficiencies, while only nine facilities to date in FY 1984 have been unsatisfactory. (See Figure 5)

Our Office of Industrial Security, International at Brussels, Belgium keeps tabs on cleared personnel assigned overseas. There are over 2700 in Europe, about 2,000 in the Middle East, 171 in Africa, 697 in the Far East and several hundred others in other parts of the world. (See Figures 6 and 7)

With respect to Personnel Security clearances, our Defense Industrial Security Clearance Office (DISCO) will process approximately 230,000 in FY 1984. This is up from 155,000 in FY 1980. (See Figure 8)

As many of you know we are gradually reducing the times for Secret and Top Secret clearances.

With our emphasis on reporting of Adverse Information there has been an increase of reports from 879 in FY 1981 to a projected amount of approximately 3,000 reports in FY 1984. (See Figure 9)

The average Daily openings and closings of personnel Security Investigations is now at about 840 cases per day. This should help reduce and eliminate our backlog. (See Figure 10)

I have one final chart (Figure 11) I want to show you and give you a little background on it. It's a little bit of a "tongue in cheek" thing. It's a balance statement. You know the Defense Investigative Service conducts investigations and works on a normal budgeting process like most government agencies. The Office of Personnel Management (OPM) operates on an industrial funding basis. They do the investigations for most of the non-DoD agencies of government. Their biggest customer is the Department of Energy. Whenever any of those departments request an investigation from OPM they get a bill and they have to pay about \$1,500 for every investigation. On the first of March OPM put out a revised reduced price list of what they charge per investigation. A special background investigation is about eighteen hundred dollars (\$1800). A regular background investigation is about fifteen hundred dollars (\$1500). We took their prices and we multiplied that by the number of investigations that the Defense Investigative Service accomplished in these categories during fiscal year 1983. If we were to operate on an industrial funding basis we would have had net sales in that fiscal year of \$234.5 million. Now, reduce from that, the actual budget of that year to run our investigation operation of 78.6 million. We would have had a gross profit of 155.9 million. Now we have to, of course, run a headquarters and that costs us \$6 million a year and I threw the Industrial Security Program in free. We run that for the taxpayers for nothing, so we reduce that from the total, to give us a net profit of 128.9 million dollars, which would have been a net profit of 55%. We had a budget in fiscal 1983 of about \$110 million and if we were to operate on a profit and loss basis, the industrial funding basis we would have been able to turn back to the stockholders, the taxpayers, \$128 million. I only put that up to show that I think you, the taxpayers, are getting your dollar's worth from the efforts of the Defense Investigative Service. We are conducting more personnel security investigations than have ever been run in the past, and we think we are doing an excellent job. Our people are working awfully hard to do that. I think these statistics emphasize that fact. Thank you very much.

DISP WORKLOAD VS ISP RESOURCES (LESS DSI)

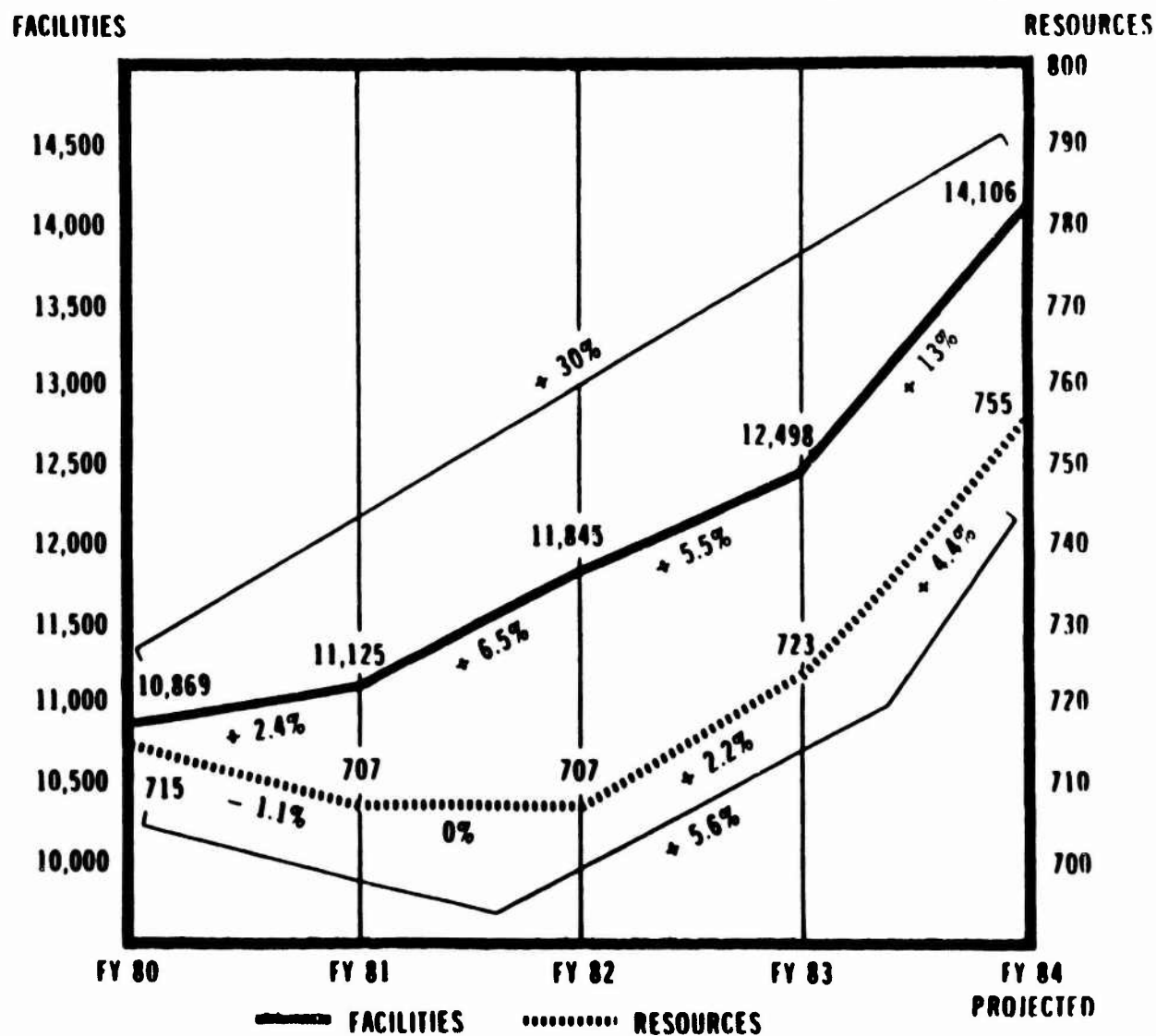


FIGURE 1

CONTRACTOR FACILITIES WITH ADP SYSTEMS

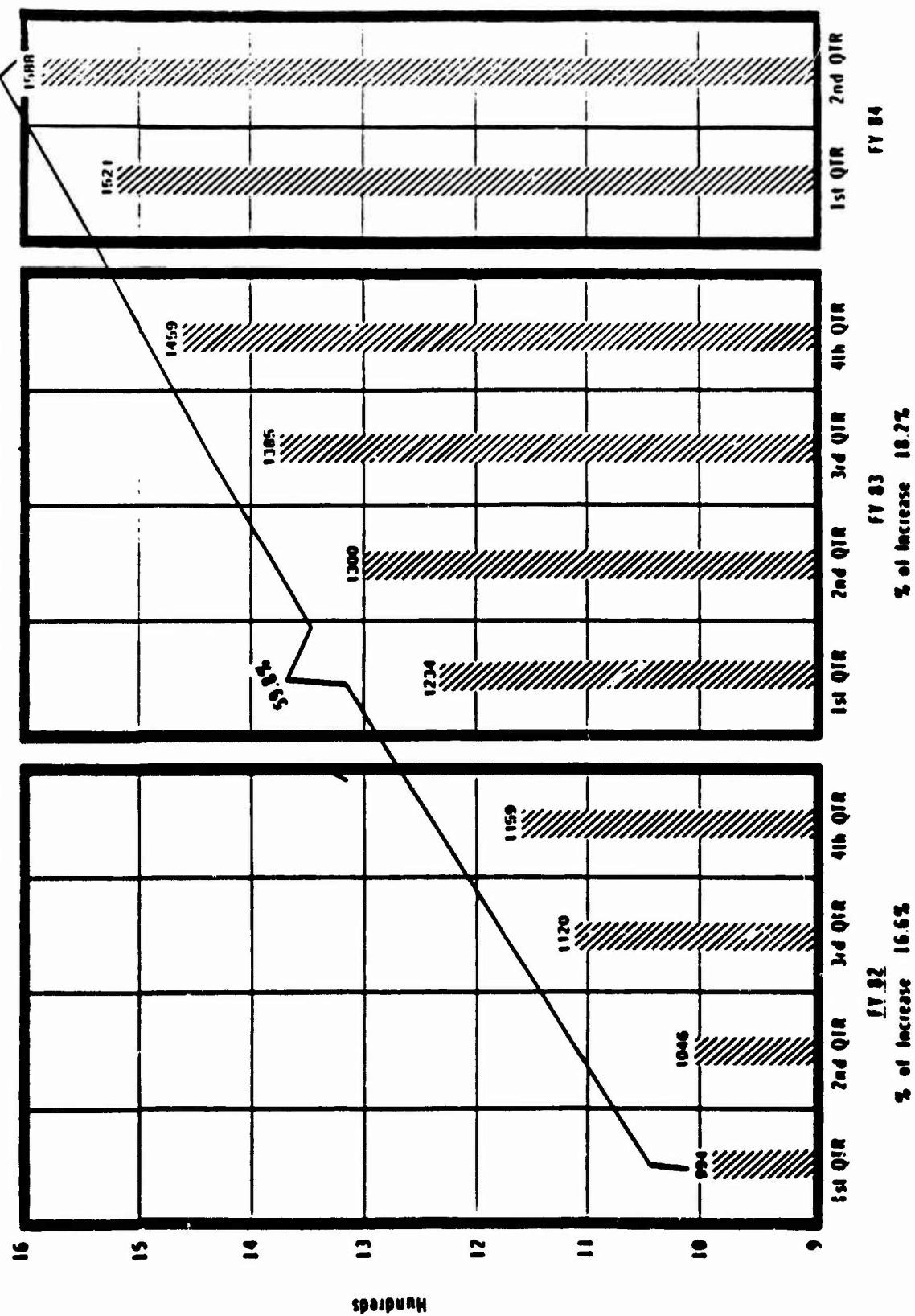


FIGURE 2

ADP SYSTEMS APPROVED AND IN - PROCESS

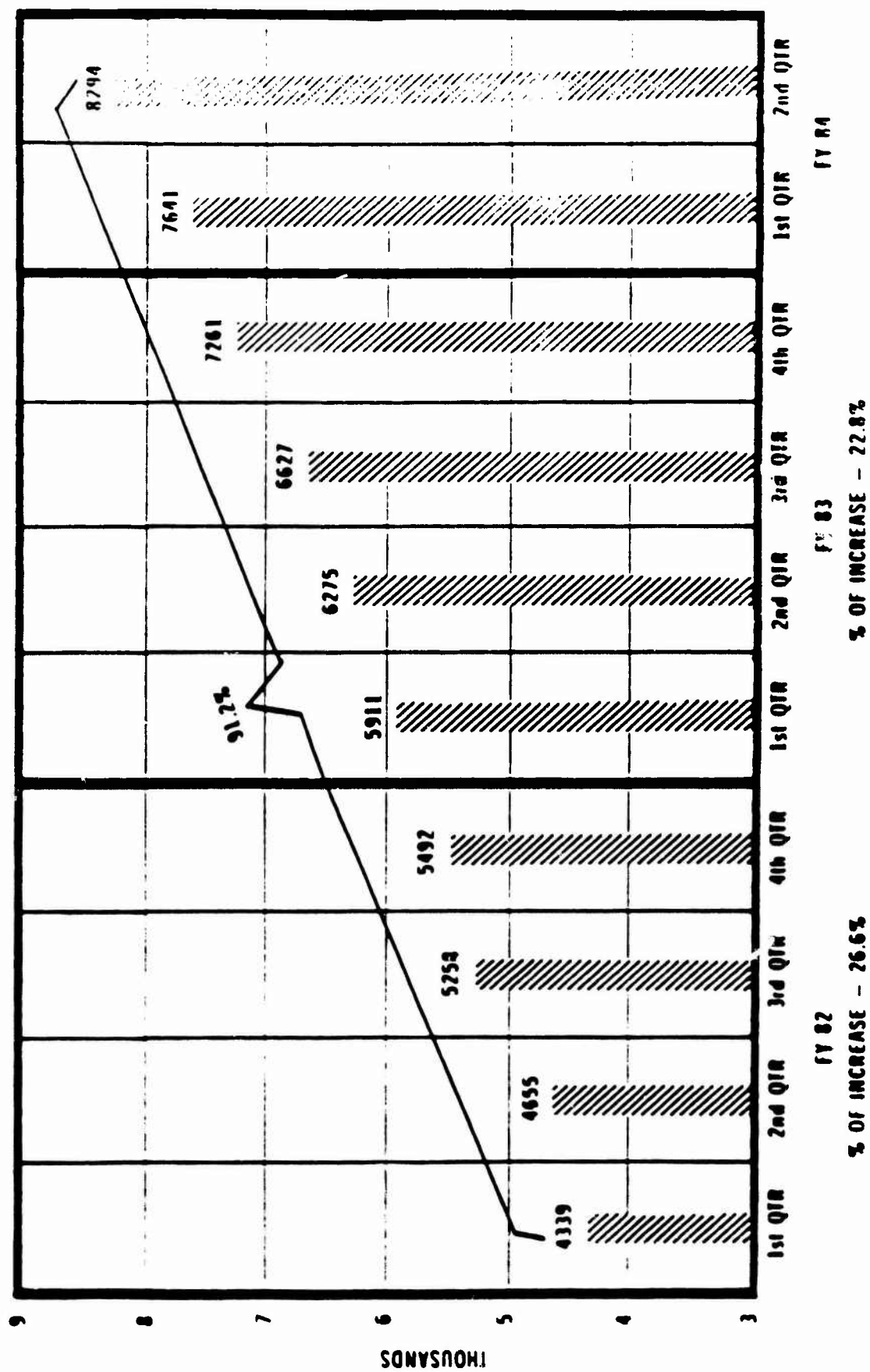


FIGURE 3

DISP INSPECTION PERFORMANCE (PROJECTED VS ACTUAL)

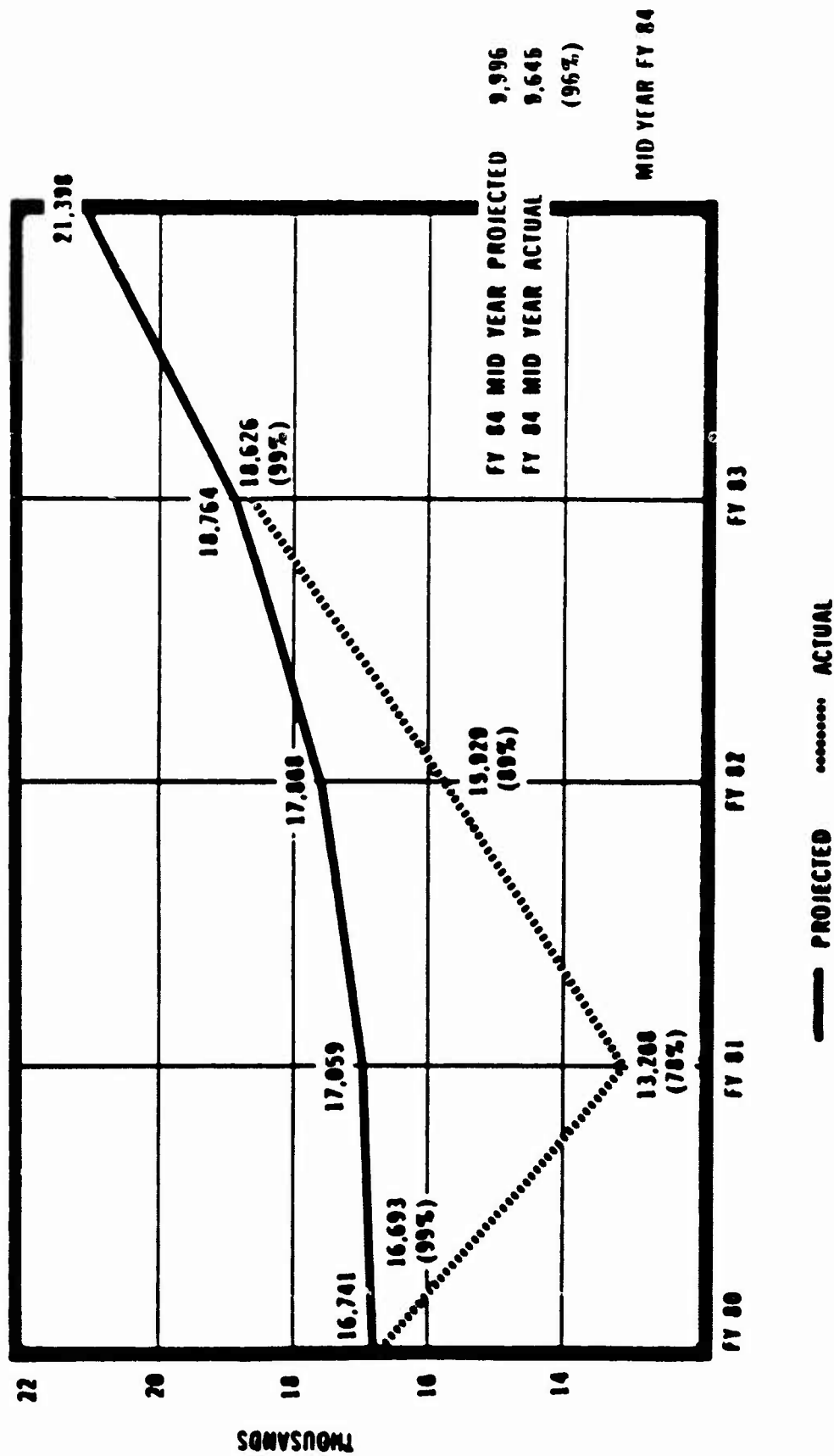


FIGURE 4

DISP INSPECTION RESULTS

RESULTS	NUMBER	% OF TOTAL	NUMBER	% OF TOTAL	NUMBER	% OF TOTAL	NUMBER	% OF TOTAL
NO DEF	5,765	43	7,441	46	8,820	47	4,898	43
COS	2,354	18	2,241	14	2,756	15	1,717	15
LOR	4,882	37	5,998	38	6,742	36	4,306	38
MAJOR	260	2	245	2	303	2	367	3
UNSAT	5	.03	4	.03	5	.02	9	.08
TOTALS	13,266	100%	15,929	100%	18,626	100%	11,297	100%

FY 81

FY 82

FY 83

FY 84

TO DATE - APR 84

FIGURE 8

VO460: OFFICE OF INDUSTRIAL SECURITY INTERNATIONAL, BRUSSELS, BELGIUM
NUMBER OF CLEARED PERSONNEL ASSIGNED OVERSEAS MARCH 1984

<u>EUROPE</u>		<u>MIDDLE EAST</u>		<u>AFRICA</u>	
Belgium	234	Bahrain	4	Algeria	6
Denmark	21	Bangladesh	1	Cameroun	1
France	42	Egypt	139	Congo	1
Germany	1,344	Israel	49	Gabon	1
Greece	82	Jordan	25	Kenya	1
Iceland	20	Kuwait	81	Liberia	2
Ireland	6	India	1	Morocco	31
Italy	190	Muscat/Oman	1	Niger	1
Luxembourg	4	Pakistan	63	Nigeria	1
Netherlands	59	Saudi Arabia	1,613	Senegal	1
Norway	16	United Emrates	10	Seychelles	76
Portugal	9	Yemen	1	Siimolia	1
Sweden	3			South Africa	3
Spain	169	TOTAL PERSONNEL	1,988	St. Helena	28
Switzerland	41	Duty Stations	206	Sudan	6
Turkey	217			Zambia	1
United Kingdom	278				
TOTAL PERSONNEL	2,739			TOTAL PERSONNEL	171
Duty Stations	911			Duty Stations	34

FIGURE 6

DISCO: PERSONNEL SECURITY CLEARANCES GRANTED

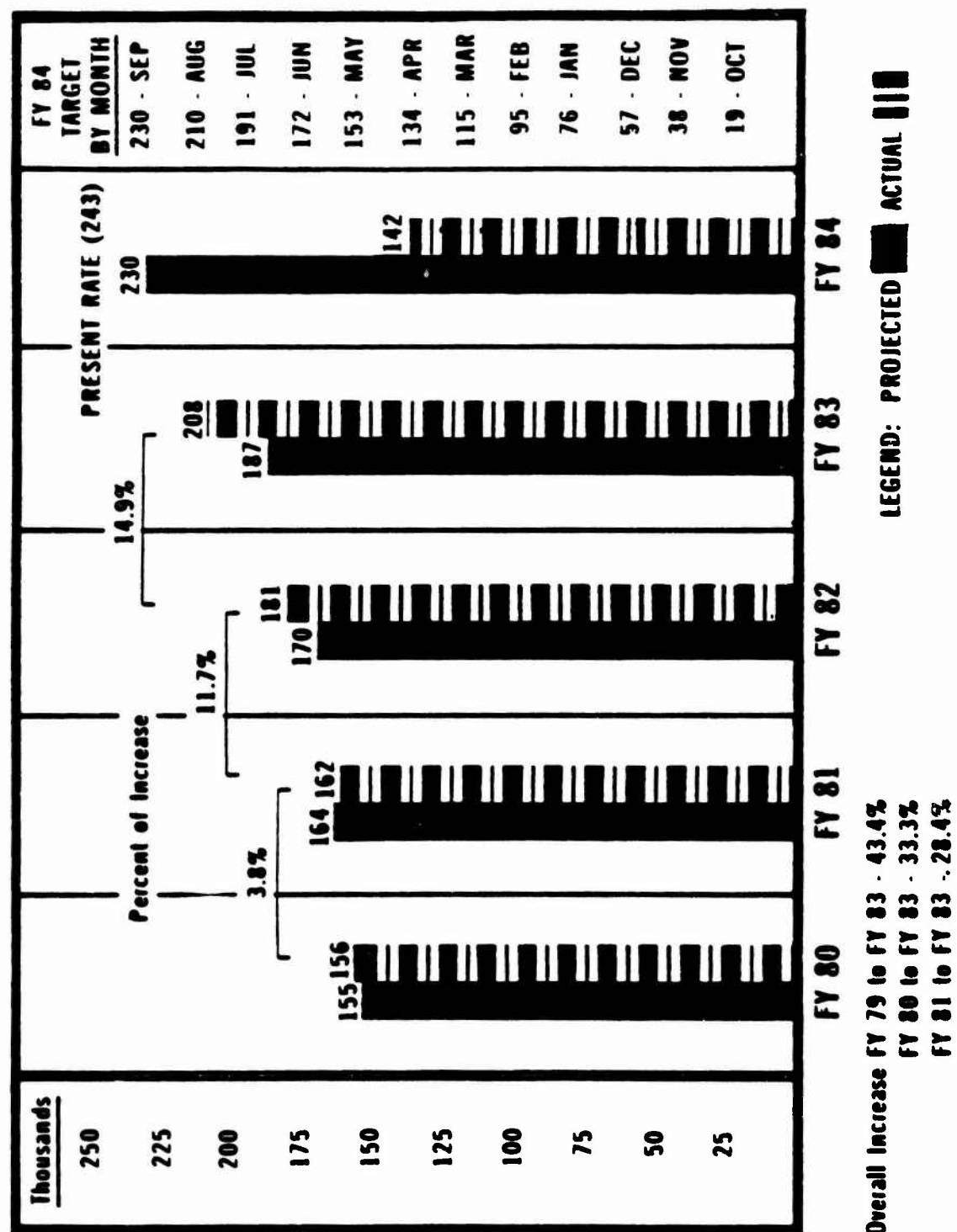


FIGURE 8

DISCO – ADVERSE INFORMATION REPORTS

NUMBER RECEIVED:					
INDUSTRY	622	743	1,257	1,372	2,352
GOVERNMENT	257	306	375	376	654
TOTALS	879	1,049	1,632	1,748	2,997
	FY81	FY82	FY83	FY84 TO DATE APR 84	FY84 PROJECTION

FIGURE 9

PSI - AVERAGE DAILY OPENINGS AND CLOSINGS

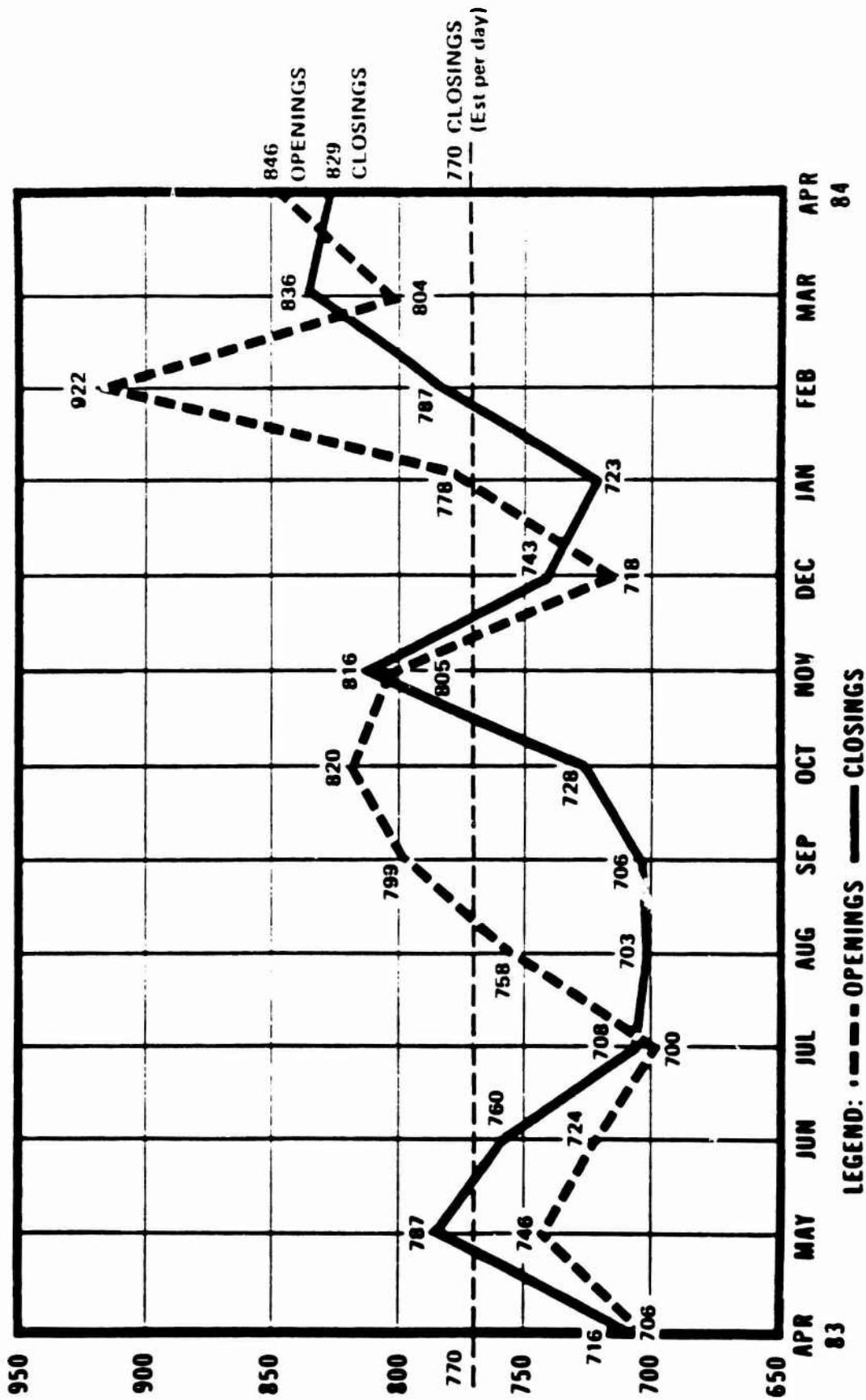


FIGURE 10

DEFENSE INVESTIGATIVE SERVICE
INCOME STATEMENT
FOR FISCAL YEAR ENDING SEPTEMBER 30, 1983

	<u>Dollars in millions</u>
SALES (DIS completed workload at OPM prices)	\$234.5
EXPENDITURES (PSI, FY83 Budget Costs)	--78.6
Gross Profit	155.9
ALLOCATION OF OVERHEAD	
Industrial Security (FY 1983 Budget Costs)	--21.0
DIS Headquarters (FY 1983 Budget Costs)	-- 8.0
Net Profit	\$128.9
Gross Profit as a % of sales	66.4
Net Profit as a % of sales	55.0 <u>a/</u>

a/ DIS can pay for the Industrial Security program and still make a 55% profit on Sales (DIS workload completed at OPM prices).

FIGURE 11

*U.S. STATE DEPARTMENT APPROACH TO
TECHNOLOGY TRANSFER*

Allen Suchinsky
Deputy Chief, Arms Licensing Div.
Office of Munitions Control
U.S. Department of State
Washington, D.C.

Mike and I have been talking about the possibility of my joining this organization. He just handed me about 25 applications, and I'm not sure what that means. He also assured me at lunch today that no one would throw anything, awaybut I've heard that before but I've got some distance on you in the U.S. Department of State approach to technology transfer. It's certainly a very timely and interesting subject these days because the Department of State has many people who don't understand and realize it is the only government agency involved with licensing commercial sales of military equipment. Many people assume that that's a DoD function, but it never has been. It's always been a State Department function, and as I'll indicate to you later and I think you will hopefully begin to understand that we have a tremendous responsibility and a tremendous effort these days in view of the greater and greater concern on what technology is being released, to whom it's going, which agency is doing the licensing, and are companies approaching the proper agency. I'll get into this also. More and more we are finding that companies are not going to the right agency for licenses and this is causing many severe difficulties. As Tom O'Brien emphasized this morning one of the biggest problems in loss of technology to the bloc countries or other unacceptable destinations is a lack of understanding on the part of corporate employees as to what the regulations are, what the responsibilities are of the various agencies with licensing responsibilities and I certainly couldn't agree with them more that this is a severe problem. I would certainly hope that your companies would attempt at their utmost to educate such people as marketeers, who as it was indicated this morning are interested in making a sale and sometimes they are not too interested in anything else but making a sale. They can cause severe difficulties for themselves and yourselves, especially in these days when many more people are watching and concerned about where technology is going. There is not a speaker on the

agenda from the Department of Commerce. They have a tremendous role also in the export and the licensing of technology that may have military utility and I would hopefully touch on a number of aspects relating to their responsibility and give you some feeling for the sorts of things that they're involved with and interested in. My primary focus will be on the State Department's role. In that regard, the Department of State's role in technology transfer is strictly, and I say strictly a control scenario. We have a control function as opposed to the Department of Commerce function which is to promote exports of equipment technology of whatever sort. This is very, very important to understand because we are frequently accused of not helping out companies in their foreign sales efforts. Why don't you have people in the embassy running around pushing the sale of military equipment in various countries? Why don't you go on trips as say the French or many others do, trips with the marketeers and be right at their side and show that the U.S. government is behind them? Well, there is some validity to this but what it would take would be a total, and I mean a total 180 degree turn in the role of the Department of State. The promoters in certain instances are people over on the DoD side. Our role again is strictly a control function. In fact it's always interesting to go to a joint meeting in Washington where there are Department of Commerce Office of Export Administration people present and Office of Munitions Control people present. You will find the Office of Export Administration people and others from Commerce running around tapping people on the shoulder from industry saying watch for such and such an opportunity, look at this and read about that. We unfortunately at times have to stand there and say but don't be so certain you'll be able to get an approval down the road should you make a sale. We are talking from State Department's perspective at something called a munitions list item for export purposes or munitions list technology. One of the great difficulties is definitional. What are we talking about when we say munitions list item as opposed to a commercial item that the Department of Commerce has licensing responsibility over. Many of the items which are used by foreign military organizations fall under the Department of Commerce export licensing jurisdiction. Many, many others fall under the State Department's license and jurisdiction and part of the educational process within your companies

is to clearly understand and make sure your people understand the distinction between those two jurisdictional set ups. If you are on the verge of consummating a big deal for a lot of dollars, say on the military side, and for whatever reason you go to the wrong agency with your license application, you're talking about the possibility of a number of months in extra delay over and above what it takes to process a license application because it may be batted around between the two agencies. Commerce may consult with us, we may have to consult with Commerce and we may have to start switching papers back and forth and you might lose a sale. You might lose a letter of credit or a number of possibilities and it makes nobody look good, quite frankly, on the commercial side or on the governmental side. So what I'd like to do is just give you a very, very brief definition of what we consider a munitions list item, meaning an item of equipment or technology which is licensable by the Department of State. Basically it's this; any item which is designed, built or modified for a specific military application falls on the U.S. Munitions List and is licensable by the State Department. Designed, built or modified encompasses certainly such items as nomenclatured equipment, equipment built under a DoD contract, or equipment which may have been commercial at one time and licensed by the Department of Commerce but now has been modified for some specific military program. This material is licensable by the Department of State and I have to stress if there ever is any question of that come and talk to us about it and if necessary we can run what we call a commodity jurisdiction case, which is a formal letter request from you for a firm jurisdictional determination on who has licensing responsibility down the road on an item of equipment.

What confuses the issue frequently is this. Your company may have an item which since its inception or invention and from the first time it was exported has always gone out under a Department of Commerce license. The end users abroad have always been commercial end users. All of a sudden you're approached by a foreign military organization and they show some interest. Many, many people jump to the conclusion that the item now has to go to the State Department to be licensed. That is incorrect, by definition that item again is not designed, built or modified for military application and is on the Commerce list. In

other words the end user is never the determinant as to who has licensing responsibility, it's the very nature of the item itself.

There is one other aspect of the factor of saving time like going to the proper agency with the license request. You're not only saving time and a lot of other potential problems nowadays because of project EXODUS which was alluded to earlier this morning where many, many companies are running afoul of customs. They're having items seized, they're having items detained, they're paying fines, they're making customers in many instances extremely unhappy because promised delivery dates have gone awry. It's not always the manufacturer or the company that comes for the export license that's the perpetrator of the crime in effect, as far as customs may be concerned or any other person or body looking at what's being shipped. Freight forwarders, another group which primarily is out to make their money and make it quickly, want to ship equipment. They have a contract with a U.S. company to ship their equipment and that's what their business is all about. Many are not the least bit concerned with the regulations other than there's a license that's necessary and somebody has to send it to customs and we think it has to be filed in some such way. Many U.S. Manufacturers licensees of munitions list equipment are finding that their freight forwarders are getting the prime company into situations where they're paying excessive fines for violations or technical violations of the regulations even when licenses have been obtained. I know for a fact that there are a number of freight forwarders that have been dropped by U.S. companies and your companies in certain instances may have had some experience with this. It's a very, very touchy situation these days, so by all means educate, not only your own people, but anybody whose peripherally involved in your export activities, be it for technology or equipment.

The Office of Munitions Control is physically located outside the State Department building in Rosslyn, Virginia. If any of you are familiar with that area, it's a part of Arlington, Virginia right across the river from the District. We've always been located outside of the main building so we can afford easier access to people from industry or outsiders so they can come and bombard us with their questions, calls and license applica-

tions and they certainly do. They've taken advantage of the situation to an unbelievable degree. I'll give you some brief statistics on that. In the Office of Munitions Control, I have working for me now four licensing officers. One of them is new and one of those positions is unfilled and it hasn't been for six months. We are now processing in excess of 40,000 cases a year by those four licensing officers. About 20% of those cases require extensive review outside of the State Department and a good deal of review within the office. They're not routine cases and everybody wants their approvals yesterday. It's a very, very difficult situation. Those four licensing officers are processing three times as many cases as were processed by this office when we had twice as many licensing officers a number of years ago. That does not make sense to me. It does not make sense to a lot of people, but that's the way it is. It's a very difficult situation and your people who have to deal with us or those of you who do deal with us, and especially those who come into the office can see what a very, very, very busy place it is. A lot of our activity is entertaining calls and visitors about cases which have gone awry. It's been a problem. The problem is that they haven't been submitted properly, often times the companies haven't provided sufficient information to enable people to carry out their review in a most expeditious manner, or the companies maybe haven't provided enough documentation or proper documentation and we have to send those cases back to the applicant without action. It's very important and again I have to emphasize to make sure that everybody in companies that are doing exporting of military or munitions list equipment understand what is required. What is required is spelled out in a document called the International Traffic in Arms Regulations (ITAR). This is, an extraction from the Federal Code. Any of you who are interested in looking at this and if you can't get a copy of the ITAR itself and you have access to a library where the Federal Code is available should look for Title 22, Code of Federal Regulations, Section 121 through 130. This, in effect, is the ITAR.

Now within the ITAR, encompassed by that document, is what I have been alluding to as the U.S. Munitions List. It's a very, very brief generic listing of categories of military equipment and it leaves open this question of interpretation which I've been mentioning and I cannot emphasize

enough the need for consultation such as calling us, or visiting us if there is any question relating to what the document means. I believe you have my phone number, we have a lot of other phone numbers which I'd be more than happy to provide to you, but I can't emphasize the need to consult. Basically we guide and advise U.S. industry on U.S. government policies regarding arms transfers to specific countries or regions. That is one of our primary responsibilities. If you want to come see us by all means call, make an appointment or if any of your people are interested or they are in Washington and they want to check up on a pending case or discuss a new case, by all means give us a call. We frequently have to direct you to other agencies or offices to seek additional guidance. On some deep foreign policy related concerns, we might send you over to the main State Department building to see an appropriate country desk officer, or regional affairs officer. As far as the technical strategic side of it it's most important that you talk to people over at the Pentagon or other agencies that may have some involvement with your equipment. We do give basic guidance as to what the possibilities are of obtaining licenses for specific countries, or regions, or groups of countries. There are times when it's best for you to send us a letter requesting an advisory opinion. These are situations or scenarios where you have a possibility or you heard that there's the possibility of making a sale in country X of equipment Y. The country is a little touchy and you are not sure if it's a sensitive enough country that because of the politics of that country or region you'd get an ultimate approval of an export license should you submit one to us. You are not certain whether or not you should expend the effort and start sending people on trips abroad because everything may fall apart when you come for that license and we have to tell you no. The thing to do is write us a letter requesting an advisory opinion. Tell us the nature of the program, give us as much information as you can as to what you foresee as the scope of the sale and the level of technology which might be released. We will send that request to the people who would be reviewing the actual request for the hardware or technical data license. In some instances send the manufacturing or technical assistance agreement that you'll be putting together, and we will come back to you with an inprinciple position which we generally 95 percent of the time can live with and will all live with.

This falls apart itself on occasions as there have been such instances of countries like Iran going down and in that instance a lot of companies lose a lot of contracts, money and a lot of sales effort. We were faced with having to revoke hundreds and hundreds of export licenses and finding out where those licenses were logged and which customs agencies even had those. So sometimes things do fall apart, but write the letters or talk to us and we can give you a pretty firm indication as to what the possibilities of gaining approval from us will be.

We process other types of cases beside the advisory opinion requests such as the commodity jurisdiction requests, as I mentioned earlier. We process the actual licenses themselves for the export of technical data or equipment. We're talking about a separate license for unclassified equipment and data and a different form for classified equipment and data. We have a different form for temporary export for demonstration purposes of equipment and another form for temporary import of equipment that's being sent back to the United States for repair or overhaul, or whatever and then is being returned to the owner of the equipment. There are a lot of forms involved, a lot of paper work involved and sometimes it is difficult to sort it all out, and then you compound that by adding the requirement for what we call manufacturing license agreements when you are going to in effect, set up a co-production arrangement with a foreign company or foreign government. We're not talking about a license form there, we are talking about a document that has to be put together by your corporate legal types and is page after page of legalities and clauses and U.S. government legislated stipulations which must be included in those agreements. Technical assistance agreements to provide, by indication, technical assistance over a lengthy period of time in a foreign country. These sorts of activities that can be difficult and confusing and when I give these seminars at the corporate levels and go to visit a company you stand there for hours sometimes going through the nuts and bolts of filling out an application, putting it all together, getting it submitted properly and that doesn't even cover it all. It's very, very confusing. But, again it can lead to some difficulties so actually it's not a bad idea if you have only peripheral involvement with those reg-

ulations to just pick up a copy and look them over. It can be very enlightening and you might discover that some of the people in your company are doing things, or have been doing things which raise some questions as to whether or not that marketer should have talked as much as he had, even under an approved license, because the scope of the license didn't cover everything. Be concerned about these things. As was indicated earlier, it's not only classified material we're concerned with. It's any material that is under some control. Meaning that there is a licensing requirement for it.

I mentioned earlier that about 15 to 20 percent of the cases we receive are sent out of the office for review. The remainder are generally routine cases which are for spare parts, or there are renewals of expiring licenses or they're for unshipped balances remaining from previously issued licenses. These are the routine ones. It's those 12 to 20 percent that take up a lot of time and there are a lot of things certainly companies can do to assist in the processing of those cases which are going to take time, which do require outside review. Here's a few examples: When you submit a case or when your company submits a case, it may take longer to do it and it may require a little digging from people filling out the license applications, but write a cover letter and tell us about the sorts of things which might be important in getting somebody who is reviewing the case to possibly move it along quicker. In other words, a very, very basic example. We receive a lot of cases in the office and we take a look at them, and we even take a look at the back up, technical data, or descriptive brochure and we still haven't the foggiest idea which U.S. service or services has cognizance over those items. If it's clear to us that it's an item that the Air Force has been involved with or had contracted for production wise, we know that the case has to be sent to the Air Force along with any other parties which may have an interest in it, but if we can't determine that, we may and we do send cases to the Air Force and Army, or the Air Force, Army and Navy and sometimes to the National Security Agency unnecessarily. It's important to give us the sort of information which will assist us in expeditious processing of these cases. If this type of information is not in the brochure, give us a cover letter and name names and tell us who at

DoD is the contract office. When the case gets over to DoD it has to go through about 15 different offices within one service. In those cases if somebody has that case and has to say something about it and doesn't have the foggiest idea what it is really all about, and if they have a name of a contact, they can move the case quickly rather than setting it aside and saying, well I'll get back to that when I can focus on it better. In other words, provide the Department of State with sufficient information to make it clear to us as laymen and we are, we are not technicians, what it's all about. Do the same thing with descriptive literature. We ask for six copies. Please give us copies that are comprehensible to us. That's not to say don't send technical data packages. Yes, if you are exporting a technical data package, we do want to see that because it is going to have to be reviewed by the technicians. But also if you have sales type literature such as, glossy brochures that put everything in laymen's terms, the people not only in my office, but the people in the main State Department building who may have to look at these cases are certainly going to understand what it's all about. Other short cuts are to come to Washington and pre-brief our people. Tell them they have a case that's coming in that's very sensitive or complicated, and let them know what it's all about. Let them know it's on its way and let them know if there are time constraints such as deadlines that you have to meet. Time constraints are another very, very touchy aspect of this whole business. You can come to Washington and tell everybody about the problems you are having in meeting a contractual date. You just put together this data package and it took you so long to do it and it has to be in the country within only two or three weeks and you know that the staffing time at the Department of State is more like one to two months. What can we do? You come and you tell me about it, or the people from your company do and you plead your case and you may go over to DoD and do the same thing. You may go to five, six, seven different people and tell them about the time constraints. That's fine, but the fifteen other people that may have to look at that case won't know about it and you probably won't know who they are to be able to tell them. Even if you did tell them, they might forget. Therefore, put the sort of information in your cover letters, by all means. Leave very little to chance, quite frankly, in this

business. It's really to your benefit to do this. Bringing this all together is the problem with project EXODUS. I know this for a fact because I've been going every few months to the custom training school in Georgia and keep talking to their people. The customs people need to be educated on this whole business. Customs has on permanent duty now in our office a customs agent. It's been very, very helpful to us and to Customs, and to industry to have this arrangement because we frequently have to suggest to people from industry who call us that they talk to our resident customs agent. The agent also coordinates on EXODUS cases, seizure cases and detention cases. He can consult with the appropriate people in the office so decisions can be made quickly as to whether or not to seize or to detain an item of equipment. On the industry's side in relation to EXODUS not only is it important to make sure that your people are dealing with the proper agency and are filing licenses correctly, your freight forwarders should be doing the same. It's important to let the people who are doing the exporting for you, such as the freight forwarders to let them know about certain types of exportation which may be a cause for some problems with customs. In other words here's an item that looks like a military radio, it's packaged like a military radio, it's painted like a military radio and yet the Commerce Department has been licensing that item for a long time and they've been licensing it for the simplest of reasons. A number of years ago you came in to us and you asked for a commodity jurisdiction ruling and you pleaded the case that this item does look like a military radio, but when you tear it apart and you get into it, it's made of all commercial components. The Department of State rule as a Commerce item means that probably no license will even be required to ship it under Commerce jurisdiction to most any destination. We've run the case on items like that and come back and have said to you by letter, yes, this is a commerce item. Fine, that was 10 years ago. Nowadays somebody may be stopped at a port of exit because of what this item looks like and the question may again be raised. Therefore, it's a good idea to advise freight forwarders or others who are doing the shipping for you about such circumstances where there is a item that may be a problem. If nothing more, have your companies talk to your shipping people and at least let them know who within the

company is familiar with the licensing of that item of equipment so that when these forwarders get stopped and are in a quandry as to what to do, at least they will have somebody's name and/or number to call. They can then quickly consult and hopefully smooth the waters without creating tidal waves. It is very important. There's no question that it's a complex business. It's important that everybody do things right nowadays and certainly if that means getting in touch with the Office of Munitions Control, Department of State. We're more than happy to talk to you and have you visit with us. I think it will be easier and save everybody a lot of problems.

We have a few more minutes and I know none of the speakers have done this, but I am certainly willing to answer some questions.

Q: What about the 1976 version of ITAR?

A: For many of you or most of you who may not know what's been going on these past few years, the ITAR that you'll pick up today has a cover on it which says 1976 version. It is the current version. There have been some supplements to that and they have been sent out as gospel in various newsletters which we send out periodically. There has been a major effort for a number of years to redo that document significantly. We've been telling industry that it's going to be ready this year and we started saying this year about five years ago. There have been a great many difficulties when we've come up with versions that we felt would be somewhat acceptable. We're deluged with contrary opinions. Industry had a chance to look at it when it's been in the Federal Register. Other U.S. government agencies have their little section which they'd like to see further modified or whatever. We've even had many comments from foreign embassies and foreign governments on this. It's taken a long, long time to rework the document. It's taken an even longer time to get it through the State Department legal office. The problem there is that there are people being called off to negotiate treaties in Greece, or Turkey or wherever and so it sits for long periods of time. I can only assure anybody that is interested that the legal people have wrapped up their effort on this and it is now back at our office. We are hopefully in the final process of getting something on the street, but I'm not going to say this year. Thank you.

ENFORCEMENT OF CRIMINAL LAW RELATIVE TO STRATEGIC EXPORTS

Joseph Tafe
U.S. Department of Justice

Ladies and gentlemen, it's a pleasure to be here today. When Jerry Ravino, the head of security at the Justice Department asked me if I would be interested in appearing before your group we readily accepted and I had the idea that you numbered about 24 to 40. You are going to be one of the biggest groups I have ever spoken to. Actually, I feel as if I'm among friends here today. In my experience at the Justice Department, in the Export Control area, I've come to know some of the speakers that are going to appear before you this week. Tom O'Brien who has already spoken today is a person I'd like to call a colleague in the sense that we have dealt with each other over the years. Jim Dearlove from the DIA is a dedicated career man with the Defense Department and I noticed Art Van Cook who was with Defense was also mentioned as a speaker, although he is no longer on the agenda. I think it is good when you are getting acquainted with someone to try and give them an idea of who you are, where you've been and what you've done. It's been my honor for the last eighteen years to be an attorney with the U.S. Department of Justice. During my 18 year career I have spent my whole career prosecuting and supervising the prosecution of criminal cases. In 1966 under President Johnson I came to Washington and at that time Nicholas Katzenbach was the Attorney General. At that time I was a special assistant to Fred Vincent. I'm going to mention some of these people who may be people you've met over the years. The first year I was at Justice I traveled throughout the United States to every major United States Attorney's office to work on a special project for the criminal division. I had a unique introduction to the prosecution of criminal cases and to see how our criminal justice system works. After that year I joined the Organized Crime and Racketeering Section. That section was primarily concerned with the prosecution of racketeers. Not marketeers but racketeers. During that time I had a unique experience to see how investigative programs start, how they develop and what type of resources are put into a program when the political emphasis comes. As you know in the Organized Crime and Racketeering area there were no strike forces back in

1967. This was what we called pre-strike force days. Two attorneys would go out in the field. I worked and covered six states. We were supposed to have an integrated program directed at organized crime. Well, we had various racketeering statutes directed at labor corruption. You would go to a state and say gee, how's your program? You would talk to two investigators who spent every waking hour on their job just collecting reports and filing various statements with the Labor Department. In a short time we came to realize that in the prosecution of labor racketeering offenses the emphasis just wasn't there. I mentioned that just to give you relevance later in my talk. After that I went to the general crime section where we had a general view of all the criminal laws, bankruptcy, extortion and kidnapping cases. I handled some prosecution and mostly supervision of actual prosecutions.

In the late 60s and early 70s, I started to specialize in bombing cases. You are probably aware of the cap bomb, pin bomb and the State Department bombings. One of the major cases that I worked on during that time was the bombing of the University of Wisconsin case in Madison, Wisconsin. In a case like the Madison, Wisconsin bombing case, which I'm sure you will recall was in 1970, a Ph.D. was doing his final papers to get his doctorate degree. Four individuals, students of the University of Wisconsin detonated a fertilizer bomb next to the University of Wisconsin which substantially destroyed the building and killed the professor. The FBI sent out what I would consider one of the greatest investigative teams I have every seen. They brought in top agents from every area of the country and the case itself was supervised by Mr. Bill Sullivan. Mr. Sullivan was an inspector in the Inspector Erskin tradition. He was respected not only by all the higher echelon in the Bureau, but by the special agents themselves. Sullivan worked that case night and day and these hundred and some agents that were dedicated to that case worked to the point where we made a prosecution in that area and we were able to solve the crime.

After that I had association with other cases such as the May Day case in Washington, D.C. where the anti-war people came to close the town of Washington. Do you recall that one? In 1973, I figured it's time to get out of the field so I decided to go to the Internal Security section. In that sec-

tion today I work under Lowell Jensen. He was the Assistant Attorney General and now he is the head of the Justice Department. I work under Steve Trock, the Assistant Attorney General. These are people I'm sure some of you may know. Our job in the Internal Security section is to supervise every major criminal investigation involving the national security laws of the United States. At the top of the list, of course, would be the espionage area. Since 1973, we've had more espionage cases than we've seen in the last 30 years. It's been a very active area, you may not realize it but, it is tremendously active. You are aware of the Camillias case involving the K-11 manual. It was purloined from the CIA and sold to the Soviets. That's a case that was directly handled and supervised by attorneys in our section, who were working with the FBI and working with the assistant United States attorneys as a partner on the team that prosecutes the case. I'm sure you are aware of the Boyce Lee case involving the theft of information from TRW. You may have read the book *The Falcon and The Snowman*. Then there was the Mattson case and the recent case involving Harper in San Francisco. He was sentenced this month and received life imprisonment. We're now handling the Smith case in Alexandria, Virginia which involves a former Army officer who is accused of giving secrets to the Soviets.

Of some interest to you perhaps is that our section also handles what we call the "leak cases" or the mishandling of classified information. Before an investigation is initiated into the field of leaks or mishandling the FBI will come over and directly deal with the attorneys in our section. The question is whether or not we initiate an investigation or not. If the investigation is initiated, the results of that investigation are given to the Justice Department. Our lawyers in the internal section make a judgment as to whether or not prosecution should go forward. Our section also handles the neutrality statutes. These briefly involve cases where anti-Castro Cubans or Haitians decide that they want to go and invade the motherland, or that they want to destroy property in a foreign country. We also prosecute those cases. We handle Atomic Energy Act violations involving nuclear sabotage and the mishandling of uranium and plutonium. I'm sure you are aware of the various matters that have come up over the years involving the New Mexico situation. When the Iranian sanctions came in it became a

criminal violation to deal with Iran during the time of the embargo. That's the International Emergency Economic Powers Act (IEEPA) so that previously when the President wanted to prohibit exports to a country he would act under the trading with the enemy act. Now of course we have what we call IEEPA. There are more controls on the President's conduct and in order to initiate an investigation you have to have the existence of a national emergency before you can have a boycott. In these periods where we initiate embargoes, they are done under the IEEPA statute and any violations of that would come to the internal section for handling with U.S. attorneys.

I tried to give you a fair idea of who I am, what our section is and what we do. Since 1982, I have been chief of a group called the Export Control Enforcement Unit within the Internal Security Section. We supervise criminal cases and investigations that are brought under the Export Administration Act and the Arms Export Control Act. We work very closely with the headquarters and the field agents in the various investigative agencies and we deal with United States attorneys of which there are 94 United States Attorney offices throughout the country. We deal directly with the Assistant United States Attorney who's working with the investigator on the case. We handle liaison with the headquarters units, and with the various other departments which would become involved including the Office of Munitions Control. I deal with Clyde Bryant and Robbie Robinson of that office. We deal with the State Department involving matters of foreign relations that are sometimes effected in these areas and we deal with Defense and the Intelligence Community, DIA, CIA and the NSA. Tom O'Brien's speech and the way he approached his speech gave me an idea to alter somewhat my presentation. Tom's key point, at least the key point that he made for me during his presentation, was that one man can make a difference. People within corporations can become effective partners with the government in making our system of controls work. Allen's speech sort of crystallized the thought somewhat that there is so much criticism especially now that the Export Administration Act is up for renewal. There is criticism of the government's activities and much of it I feel is ill informed or motivated from reasons other than what I see as clear thinking. The Export Control System is geared, as I see it, to one purpose. The licensing

under the Export Administration Act only has one primary purpose and that is to assure strategic goods being licensed are not diverted to the Soviet Union or to some other destination that would be against our interests. So that when a manufacturer has an item that he wants to sell through a company in France, or England, or West Germany it seems to me as a theoretical proposition that this ought to run fairly smoothly. If everybody is doing their job the way it should be done, then all these delays and confusions and problems should be avoided and it really bothers me that there are those who will attack the whole system because a license was delayed or that there was a problem here or a problem there. All of you people have good educations and you've seen people who are otherwise very intelligent and analyze a problem to death where it involves their vital interest. However, when it comes to national security and vital interests of the government and the vital interests of the NATO alliance, if you're ready to throw out the whole system because there was a delay, it seems to me that you've got to attack the problem. You know if a fellow in Washington wasn't doing his job right, that's the problem. Go after him. If a guy in licensing is screwing things up and he's not getting his job done, go to the highest level and get the matter squared away. The same within your own organization, if your people aren't furnishing the right information, or if it's causing delays in Washington you can't expect the guy to be a clairvoyant. If you're not furnishing the proper information then he's not going to be able to act on the license. There's a lot of rhetoric and sloganism. You know free trade versus isolationist and a lot of it comes down to if the system would work the way it's supposed to work there wouldn't be the problems we have today. The concept of reexamination that Tom brought up is something that we all have to do and we really have to work at it.

When I got into the Export Control area it was sort of by happenstance back in 1978. At that time the Export Administration Act was being handled by another section within the Criminal Division. A call came over from the National Security Council that they were doing a Presidential Review Memorandum. They needed an individual from the Justice Department who could be a representative at a fairly high level on enforcement matters. All the high level guys were tied up so they sent

me. So I went over to this meeting and they passed out a document which was a draft Presidential Review Memorandum that I understand was something that was done to update studies in the area. When it got down to my part, the part that I was supposed to look at, it said enforcement of our criminal laws in the export control area is doing fine, it's a good program. So I thought, well I ought to come back to Justice and find out what kind of program the government has. I came back and I called the attorney in the section that handled the statute and got a rundown and he said, oh well, we get an export control case under the Export Administration Act about once every two years and the investigative agency that investigates, they got about three or four investigators out there I think. So I went over to our people and I thought that maybe we ought to do a little study in this area. One of the first things I did was get the statute changed from that fellow's section to our section. As a good bureaucrat you can't operate unless you have statutory authority. We then started asking questions. We went around to the various agencies and found that there was a group of people who were dissatisfied with the way things were being done. The professionals within these organizations knew that we didn't have anything that approached an effective law enforcement system. The Commerce Department said, look we've just come through a period of détente with the Soviets and everything seems to get licensed. In any event we don't get any money; therefore, we can't hire investigative agents and we don't have much of a program. The intelligence community people said, well you know collection of this kind of intelligence is sort of a byproduct of other collection activities and we have other priorities, is this a problem? A small group of people started to ask the question and put some doubt on what they were going to conclude in this study. The decision was made to form a study group specifically geared at this problem. How were we doing in the area of export controls, what were the problems, how were we doing the job? Ed O'Malley, who is now the Assistant Director of the FBI intelligence was designated as the man who would lead the group. To the credit of the individuals who showed up at these meetings, it was somewhat like a profile in courage. You can imagine a fellow who came in from a department that wasn't doing anything and sat down and said, hey, our operation is a joke, we're really not doing the job. I've been

telling them over there for years that we haven't done the job, it's a profile in courage. Actually he still works there today and has a good position. The same way with the intelligence community and they said, well, we've been watching this stuff go for years, but we didn't really realize that you all had any investigative interest in doing anything about this, so as far as disseminating export control information that we collect to the investigators or the prosecutors that could do something about it we didn't think that was something we could do, sources, methods and problems like that. And so on down the line, each agency had it's own view of what the problem is. You dealt with the State Department and they are thinking about foreign relations. This may cause some problems with our allies and the Department of Defense will say, well, we see the problem, but I think Jim Dearlove was the only one talking about it. In any event, we wrote the report coming out of that Committee, laid out what the problems were and sent it forward and like a normal government response they said, we have a real problem here. We better form another committee. So another committee was formed. When this administration came in, after a shakedown period, they started to get interested in export control. The intelligence community was tasked to do a study of the whole area. The results of that study began to filter in during 1981 and the final report was published in 1982.

The same time during 1981 the Commerce Department knowing that it was under the gun to make cases got out there and started beating the bushes and they made several good criminal cases in the export control area. These were made in the Los Angeles area. One involved a fellow named Tony Mulluto. Mr. Mulluto became very wealthy exporting computer parts, integrated circuit manufacturing equipment and communication equipment through West Germany and Switzerland to the Soviet Union. Then we had the Spar case in 1981. That case showed that laser mirrors which were important to scientific military research and development had been exported by a small manufacturer of copper cool laser mirrors to the Soviet Union. So we started to get an awareness of what the problem was, not only from the intelligence community but from the cases that we started to develop. The small group of fellows who were interested in doing something in this area had to answer, what's the problem? There was an actual denial of the existence

of the problem up until that point. Those who did not want to see anything done in this area were like the chicken and the egg. If you don't have the cases, what is the problem? Until the intelligence community came along and told us that here's what it is, here's the scope of it, here's the dimension of it, then, you know as lawyers at the Justice Department or as a fellow over at the Defense Department that's not in DIA doesn't have the wherewithall, the capacity, the resources to be able to answer that. Just being people around the business awhile we knew that wherever you have a law and you don't have investigators out there trying to make the cases and developing the intelligence that it takes to make cases, you're not going to have any cases. Therefore, like the Labor Department investigator that I met back in 1967 said, we don't have much of a problem in this area although I don't get out of the office to find out whether we do or we don't. The study that was done by the intelligence community is now published. Many of you no doubt are familiar with it, it's called the Soviet Acquisition of Western Technology. Mr. Anderson and Tom O'Brien have touched on salient points in that study. In essence it tells us that the Soviet war machine is being backed up by Western technology, that 70 percent of the acquisitions of strategic technology being made by the Soviets are being made by the KGB, GRU and the sister Soviet intelligence services. There are two thousand collectors from the Soviet bloc nations out there trying to acquire strategic technology. The weapons systems projected into the 80s and the 90s that the Soviets have on the planning boards now are relying on a steady supply of strategic technology from the West. Just think of that. They're planning their systems based on technology that they don't have, that they know or anticipate that they will acquire from us. So in 1981, it was a year of reexamination, a year of here's the problem, let's do something about it. At the end of 1981 the U.S. Customs Service started the EXODUS program. EXODUS means that they have a credible force of investigators out there now. They are out there trying to develop export control intelligence that will make cases. They are coordinating with the intelligence community to use our vast resources of intelligence that we gather around the world to see if we can't pinpoint who the diverters are and what they're up to now. In 1981 Admiral Inman from the CIA reorganized the intelligence communities efforts and made it a high priority to

collect intelligence relating to the Soviet acquisition efforts. They ordered the various agencies within the community to report and deal with the investigative agencies on the basis of trust, confidence, and to develop ways and means to utilize intelligence information and at the same time protect the sources and methods that went into acquiring such information. At the Justice Department we formed, under the chairmanship of Lowell Jensen, who's now the Associate Attorney General, the inner agency working group on this problem. It's a group composed of all the investigative agencies. Members of the intelligence community, Defense and State, get together periodically to meet and discuss how we can make our enforcement system more effective. This group has a working group that meets regularly when we get together with just the investigative agencies with various input from other sources to develop strategy and tactics to meet what is becoming a more sophisticated run at our technology being made by the Soviet intelligence services. As we get better, they get better, or as they get better, we have to get better and we are constantly working at getting better. Tom O'Brien explained to you the FBI's DECCA program, and 13,000 defense contractors in the United States export control have been added as an ingredient in that program to sensitize industry to the problem. Foreign counter intelligence investigations by the FBI in the area of technology transfer have increased. The FBI does not have investigative jurisdiction over the specific violations over the Export Administration Act or the Arms Export Control Act. However, where there is a hostile foreign intelligence service involvement in any violations of law, then the FBI can conduct foreign counter intelligence investigations. The FBI develops good intelligence and where it does not wish to pursue a specific statutory offense, it refers that matter to the U.S. Customs Service of the Commerce Department. So as you can see in 1981 and 1982 there was an across the board up and down approach, a change. The political will and the leadership was there and they told the investigators go do your job. You know how to do it. Devise a program to address the problem. So, the actions were taken. Once the political decision is made, you ask the group of professionals to go out and do the job and they'll do the job. The problem prior to that time had been an identification of the problem, but the decision to make this an important area of law enforce-

ment was not there. But, it is just not law enforcement, it's a whole approach your Federal government has taken to the area of strategic exports. It's approach is across the board at various policy levels with regard to licensing, what we license and what we won't license. As you know over the years there have been many mistakes made in terms of what we have directly licensed to the Soviets.

We just handled a case in our office that was prosecuted in the District of Columbia. The defendant came in and plead guilty this month and was sentenced to a \$3.1 million fine. The defendant was ably represented by Edward Bennett Williams and in fact the government had recommended an appropriate fine of a million dollars. The judge imposed a fine of 3.1 million dollars so we were happy. That case involved the licensing back in 1977, 1978, and 1979 of an air traffic control system to the Soviet Union. It's another example of the assurances that are made that cannot be relied on. A Swedish firm contracted with the Soviets to provide what was supposed to be a civilian air traffic control system. There was a significant amount of U S parts that were going to be involved; therefore, we had the right to control and to license what the Swedish firm was going to do. The Swedish firm came in and made all kinds of assurances, there were about 14 conditions that were laid down before the license was issued to protect against what happened, which was that the Soviets were provided with software and technology that enabled them to convert a civilian air traffic control system into a military air traffic control system. At least the capability is there. It's interesting in that the Soviets don't want to come to the Olympics. Actually the whole purchase of this air traffic control system from the West was initiated because of the Olympic games that were going to be held in Moscow, at least that was the representations that were made. So in any event there is a new awareness that representations made to us through our allies as to what the Soviet intentions are have to be approached rather skeptically. I think our record since 1981, and what we're doing in the area today means that we do have an effective enforcement program for these laws which effect our vital national security interests. There have been 50 export control cases since 1981. More than a third of these cases have involved direct exportation to the Soviet bloc.

Other cases we count involve other vital interests of ours which are the protection of our interests in preventing the Libyans from getting C130 type material, and preventing the Iranians from getting materials as they deal with Cuba. Also in that number of cases are some Arms Export Control Act cases which is a straight weapons deal. Our renewed emphasis in this important area of the law has also important benefits for U.S. industry. As you are no doubt aware, in 1982 the Federal Bureau of Investigations initiated an undercover operation in the San Francisco area. This undercover operation was designed to detect some of the large scale thefts in the Silicon Valley area. The word got out that this store front was interested in purchasing and selling integrated circuits, computers, computer documents and things like that. The next thing the FBI knew they were dealing with representatives from the Hitachi Corporation in Japan. First there was just the middle man, and then they started to get the executives from the company. In any event that case involved the conspiracy to acquire \$625 thousand dollars worth of IBM documents, tapes and computer components. These were top of the line state of the art computer equipments that IBM was developing and it would come out in the next models. That case involved interstate transportation of stolen property. We in the security section worked with the U.S. States Attorney's office in putting that case together, determining whether or not they had gone far enough and whether or not we had probable cause to prosecute. As you can see the message is there. The foreign competitors that come to the United States and try to steal our corporations' advanced technology can expect to meet the FBI or some other investigative agency and in the same way it gives solace to companies to know that your FBI and other investigative agencies are going to be there to protect your proprietary information from thefts by domestic competitors. We're all for free, energetic and open competition, but when it comes to stealing the other fellows products I think we all expect to be protected. So as you can see there are important spin off benefits from our enhanced investigative program. Today I've talked mostly about what we do here in the domestic area.

We also have a large effort ongoing in the international area.

It was decided at the summit in 1981 that there should be a high level meeting of the COCOM

countries to rededicate themselves to the proposition that we all have to do a better job. We approached our allies with our program, what we are doing, how we have examined the problem and how we have attempted to meet the threat that the Soviets have advanced. We know what we went through and we know what their problems are and we know that some of them are a long way away from what we would call an effective enforcement program. Having this broad overview of where we were, where we are, where we are going and listening to some of the current things that come up including the debate on the Export Administration Act like we ought to do away with COCOM licensing. That's a good one, that comes up and I'm sure you have heard it within your own companies. Why should we make an exporter in West Germany tell us what the ultimate end use is going to be, describe the equipment and everything like that. As I say our licensing system is our only way of knowing where the product is going, where it's supposed to be and hopefully we can check up and make sure that it got there. If you do away with COCOM licensing you are pushing your program across the sea and you are going to rely on Frenchmen, Englishmen and West Germans to enforce your strategic export control program, and gentlemen, it is not going to work if we do it that way. Our dealings with our COCOM allies and renewal of our customs attache contacts in these foreign countries has paid off significant benefits for us. You are no doubt aware of the case that arose in November 1983. Custom service received information that a vessel had left South Africa, was on its way to the Soviet Union, would make a stop in Hamburg, Germany; Malo, Sweden, and then go into the Soviet Union. Custom investigators came over to our office and they said we have this information and we're dealing with the West German customs people. They would like to take some action but the problem is this vessel is going to come into a free port. West Germans do not exercise traditional law enforcement jurisdiction over the free port of Hamburg. Therefore, they are going to have to go to their justice people to get a search warrant. What can you do to help us? Well at the Justice Department, fortunately, we have the Office of International Liaison. I always get their name wrong, but in any event it is a group of attorneys that deal with our foreign counterparts; the Justice Department counterparts in the NATO countries. We got together that night and worked through the evening to develop

the information, the probable cause type information that the customs have. We satisfied ourselves that they did have good information and that indeed the computers that were of U.S. origin had gone to South Africa and were indeed on their way to the Soviet Union. These were VACs 11782s. Pretty good stuff as I understand. In any event our counterparts in Germany were convinced that we had good information and although they didn't go into the free zone, they would take action and go in and examine the vessel. They did, the VACs and the peripherals were there. They were then loaded off onto the German docks. Subsequently, they have been returned to the United States. We are conducting a rather active investigation into that case which involves as the principal subject a fellow named Mueller, a don of the export trade in West Germany. Actually Mueller is sort of an interesting case study. This fellow was prosecuted and indicted in California, back in 1976. An associate was indicted in Baltimore on an Arms Export Control Act in 1981 and he was rather well known as being an exporter of strategic goods. But, when the heat came on in 1982 and the West Germans started to get interested in his operations, he moved them lock, stock and barrel down to South Africa. Unfortunately, our intelligence wasn't good enough. We were actually licensing the computers from the United States. Digital Equipment Corporation computers were being licensed to South Africa based on a rather good front that he put up. In any event through that system we recovered \$3 million dollars worth of equipment. Seven million dollars worth of equipment had been exported through that route so \$4 million is still missing.

Let me conclude my remarks. I think that from what you have heard today you know the problem and if you really think about it, the Soviets are challenging each and every one of us. The challenge is clear, it's there. It should be accepted. Whatever part we play in the whole system it's imperative to use our best resources, our best judgment and our best efforts to make the system that we have work. It protects vital interests. It's in our own vital interests to make the system that we have work. I'm confident that the government, private industry and our allies working together can meet this challenge that the Soviets have presented to us. We can deny them a supply of strategic equipment. We can deny their expectations and we will do it. We will work together doing it. Thank you.

OPSEC FROM THE STANDPOINT OF AN IMPLEMENTER

Thomas Conner
Dept of the Army
Communications & Electronics Command

It's a pleasure to be here and I appreciate the opportunity to come in front of this group. I must highlight the fact that I certainly do not speak for the Department of the Army or DARCOM headquarters, or the CECOM commander. You are going to hear today personal observations made during my limited experience in the field of operations security. (OPSEC) The thoughts and ideas expressed here today are our solutions to these problems as we envision them and they certainly are not set in concrete. In that regard I solicit your comments, helpful suggestions and yes, most especially your criticisms because it is only through feedback from knowledgeable individuals that we have any chance of trying to strengthen and improve our program. So if during this presentation you should happen to disagree with something then challenge it. If you have encountered a similar problem and have a somewhat different solution, then by all means please offer it. In short, I'd say, let's try and participate so we can learn from each other. I am a security specialist with CECOM, the Communications and Electronics Command, a DARCOM activity at Fort Monmouth, New Jersey. To give you somewhat of an idea of the magnitude of the problem that confronts us, I would like to give you a thumbnail explanation of the areas of responsibility. We in the security office provide total security support to some 15,000 military and civilian employees, in a command that has the dual responsibilities of readiness as well as research and development. In that regard we support 12 separate program managers, four army centers devoted to research, three joint service tenant activities, a separate and distinct research and development center and a commodity center for all electronic equipment. Now, in the commodity or readiness side of the house, we are responsible for all communications and electronics equipment in the army inventory and that takes the full range from flashlight batteries to satellite communications systems. It takes in the spectrum of radios, radar sensors, GMA and electronic warfare devices. On the business side of the house our procurement director placed contracts during fiscal year 1983 in the amount of 1.8 billion and our projection for

1984 is to go over 2 billion. On the research and development side of the house to include the PMS and centers new development and technology in the use or application of that technology are our chief products. So you might say it might be a little hard to keep the boss happy, especially in a command that size when he takes the form of seven different General Officers. So when Mike asked me to speak to you about OPSEC implementation I hope you can understand why I was somewhat perplexed and when I asked for further guidance I was told that I should address the topic in a general way, highlighting some of the areas of mutual concern. Well, further examination of the problem revealed that I was to go to this conference, speak to you as a security specialist but talk to you in a general way. We all know and I will certainly prove today that a conference is something that starts at 9 o'clock sharp and ends at 4 o'clock dull. A specialist is someone who knows more and more about less and less until he knows everything about nothing and a generalist is someone who knows less and less about more and more until he knows nothing about everything. So today during my presentation will endeavor to tell you all there is to know about nothing. I will do it in a very specific way and before I'm through I promise that you will be bored. I'm sure that giving advice on any particular subject is usually a thankless business, and I assure you that I will not venture forth in that direction. You know when it comes to giving advice I've always kept in mind the unconsciously profound summation written by a small school girl. Here's what she wrote. Socrates, she wrote, was a greek philosopher who went about giving people good advice. They poisoned him.

At this point I have to break tradition and give you some of the philosophy of our program and even some of the lessons learned now, rather than at the end of the presentation so that hopefully you can see how the philosophy is permeated through our program and how the lessons learned have modified it. To begin with, we at Fort Monmouth understand the purpose of OPSEC is to protect all types of information, both classified and sensitive unclassified aspects. However, considering that the systems that we had were already in place for protection of classified information, we took the stand and felt that the bulk of effort in the OPSEC area should be to identify and control those sensitive unclassified informational aspects relating to our plans, pro-

grams and projects. Now in order to accomplish this our philosophy took on several axioms.

First of all not all information requires protection. To say that every bit and piece of information about every program and project is sensitive and requires protection simply isn't realistic or attainable. An additional biproduct of that frame of mind is that as soon as you tell someone that you have to protect everything, you almost immediately lose creditability. Therefore we chose to establish those essential elements that we believe required protection and set about on a course of implementation, or like the highlight that we did not consider this a full back position. We honestly believe that in our programs and projects that every bit of information is not sensitive.

Secondly, the information that requires protection can change during the course of a plan or project which in turn changes the degree of protection afforded that information, and third and most important, where we receive the most criticism from, regardless of the amount of regulatory guidance, we believe that OPSEC comes down to a subjective decision at a particular point in time. Let me illustrate these points by way of an example. In early 1982 our office was involved in giving support to a mobility exercise and in the course of that problem a message was released by our headquarters to several Army posts requiring supply actions. The message called for radio and electronics equipment to be delivered to various Army units at a specific place at a specific time. Again, let me emphasize that this was exercise traffic and did not relate to a real world requirement. Well, within two hours of transmission of that message we were in receipt of nastygrams from the local MI group, the MI supporting battalion at Fort Meade, DARCOM Headquarters, several who were involved in the exercise and even our own local control group. To make a long story short they were out to get the fat Irish kid. They said, Hey what are you doing? Well the summation of their concern was that this particular message had not only seriously violated all OPSEC principles by giving equipments and where they were going in units, but the information provided over unsecured communications bordered on the compromise of classified information. Well, an analysis of the situation provided the following information.

During the play of the problem the following actions had already been taken. We had our sense of urgency and now we had to go and complete it. The President of the United States had called a news conference in which he stated that there was going to be mobilization. Subsequent to the conference the Department of Defense released the identity of the units to be mobilized, and third the various departments under DOD issued reporting instructions for the individual units concerned. Well, taking into account the fact that all this information had been broadly and openly publicized just how sensitive was it for us to say that we were going to give these units radios. The point thing, that to take any piece of information in total isolation without relating it to other known pieces of information cannot and will not result in an accurate decision regarding sensitivity. Now, this can also turn around on you, consequently in the play of a problem the radios were delivered, some of which were in an unserviceable condition and they were returned. The unit subsequently deployed. We sent a message to the service depots asking them when are you going to resupply these radios. That particular message was sent, although unclassified, over secure communications. The reason being that at this point in time we felt to divulge that information would reveal a potential vulnerability to the unit. Consequently what I am trying to say is that the same piece of information dealing with the quantities of radios took on varying degrees of sensitivity when analyzed in conjunction with the information available, and you analyze this piece of information with the information available and make a subjective decision for that isolated point in time.

Okay, now that we have gotten through the principles let's examine how we tried to implement. First I have to kind of tell you where we were, where we are now and hopefully where we are trying to get to. It all started in 1979 when our inspection team came in from DARCOM headquarters. They referred to us as the security support activity. The gentleman in charge was a fellow by the name of Chuck Cooper and once again as in every year we found ourselves to be the two biggest liars in the world when I told him I was glad to see him, and he told me he was there to help me. During that phase in time they came to look at our program, to look at our training and specifically OPSEC. Our philosophy at that point

in time was to individually teach or in a group teach our security managers. Each one of our PMs, laboratories, directorates, etc. has a security point of contact, a security manager if you will, and our philosophy was to teach them and they would also teach the other people. Well, through the inspection process it was learned that the level of understanding and appreciation for our program was almost extinct, or non-existent and the real crowning blow came when Mr. Cooper was talking to a gentleman, a marvelous scientist who personally worked on the satellites. They were sitting in his office drinking coffee, talking about security issues and Mr. Cooper said, Dr. now tell me what do you really think about OPSEC? The doctor pondered for a second, took a sip of coffee, put the coffee down and then he said Mr. Cooper I think it's totally unconscionable the amount of money those people are getting for oil. Okay, our objective was clear and we certainly had out impetus for higher headquarters and we were to train the work force. But there were many questions that remained not the least of which were, who do we train, how do we train, who does the training and who trains the trainers. In January of 1980 we set a course on our chart to start a training program to reach the people. Now in any security training, and this one was adopted to OPSEC, we felt it most important to be current. Our problem was that our library of films were back in the 1942 issue on World War II and how to change combinations. So we had to spend an awful lot of time to try and bring ourselves up to speed. Certainly we had to be accurate. No one expected us to get this done in a 30 day period. We started in January of 1980 and our initial goal was to try and train the work force in nine months and then go through with a refresher for three more months. We were going to spend a whole year in trying to implement this program. For a hundred years everybody has been giving security education and I don't know where it came from but everybody feels if you're going to give a class it must last an hour. We felt that was wrong, we felt the most we could hold anyone's attention was 30 minutes. So far I've held yours about 10 and I've lost half of you, so I don't know how long we can keep up with this 30 minutes. We tried to mix it up with a lot of visual aids but we certainly did not want to go over 30 minutes in any of our presentations. Be pertinent, certainly; don't give the wrong training to the wrong people, don't take mid-managers and tell them

how to mark a document and don't have high level supervisors go over the accountability system. They have people that do that for them. Resources was a big problem, not only in the material concept but in people. How are we going to cut this time out of our existing budget. We had to implement a program, and we also knew we had to do it with no new money and no new people and address different categories of people and audiences. The reason that we broke them into categories was we certainly didn't want to talk to mid-managers about the things the secretaries should be learning. In order to make the training pertinent to them and to make it worthwhile you cannot give the same training to everybody. Now this is an axiom that's been brought out and reinforced by Joe Brown in a lot of his presentations and it works. Don't give the wrong training to the wrong people. The real challenge here is these topics are not new. Certainly we had a separate topic dealing with OPSEC as a commodity, but the real challenge was to interweave OPSEC in all other categories. We honestly believe that if you have it as a stand alone program it will fail. It must be interrelated with your other programs in order to see the value and the importance. What we did was bring all the security managers in for a quarterly meeting. We built up a video tape library that now has approximately 35 tapes in it. They've all been current, they are all in color and they all run about 12 to 15 minutes. We show a video tape on a particular topic. From that topic then we'd give what we call a mini course. For example Jim Mathina has done fantastic work with marking documents. We took that course and broke it down into about eight different courses. The point being we didn't want any course to last more than 15 minutes and we wanted each course to have approximately 30 viewgraphs to keep it snappy, to keep it moving. From that 15 minute presentation and viewgraphs we would develop a one page desk top guide. For example, portion markings would all be on one page, how to remark a document in conscience with the new executive order would be another page, but it would be a one page desk top guide. We would also distribute a bulletin. It ran about 10 pages telling them what's happening. Also in the bulletin we would have class schedules. When we first started out with security managers we only asked one thing of them and the thing we asked them to do was to go back to their activity and to send the people from their

activity who would get something out of this training. We didn't want everybody from their activity because in some particular phase of training it wasn't supposed to be for everyone. So don't make it mandatory for those people who really don't need it. We of course have discussions during the meeting to try and get feedback, questions answered, and when the next meeting would be. On a quarterly basis we picked the topic and trained the security managers during that quarter. We ran classes on that topic and then the next quarter we would start up with a new presentation. The bulletin that went out had current topics in it dealing with security, any regulatory changes, any new things happening in the area during our inspection process and if we could pick out trends of things happening, we would also incorporate that. We considered this security awareness and we tried to get OPSEC into it. We published approximately 300 different one liners that go in the daily bulletins. We had 50 different posters dealing with OPSEC. We also had an OPSEC booklet which is basically a how to document saying what is OPSEC and how do you get into it. A specialized survey would be that the areas of concern in one PM aren't certainly the same as it would be in a directorate for procurement and our security education ran this full gamut. The point was we saw a crying need that you cannot fill the bill with one annual training session and you must break it down into categories that will fit the people that are getting the training. Even with all this training that went on we still found people, believe it or not, in our command that did not like OPSEC, didn't believe in OPSEC and didn't think that OPSEC made any sense. I was crushed and I must admit that it really isn't the easiest program to sell, but if you stop to think about it, it's really not all that hard. In fact it's not really any harder than some of the things that Bill Johnson is doing to protect his new car. Bill did just get a new car, he's got a nice new convertible and just the other day in Alabama it was sitting out in the parking lot on a beautiful sunny day. Bill was sitting at his desk and a couple of people came in and said Bill I love your car, but it's going to rain. Bill said I *didn't* know that. So they called, got the weatherman and he said thunder showers were on the way. He said, no it's not going to rain. Heard it on the radio, thundershowers, maybe even a small tornado. It's not going to rain. So it's obvious with that convertible the threat was certainly doc-

umented. The vulnerability is obvious and the counter measures wouldn't have been expensive. The point is everybody told Bill it was going to rain, but Bill didn't see the rain so he didn't put his top up. They started to make a fishing hole out of it because it filled up with water and they had fish in it and everything else.

The point being if you start talking about OPSEC and people come in and tell you that there is a recognized threat whether it be HUMINT, SIG-ENT, etc and to sit back and say well they haven't got anything from us yet. I think we have to act a little faster than that. The problem is that everybody can tell you war stories and technology transfer and how things are leaving, but how are we going to stop it if we don't use OPSEC or something in the area of technology transfer. I'm not saying that OPSEC is the total answer, But I think there are some concepts in it that can be adapted to almost any area. So really through education and continual follow up, hopefully our OPSEC program has reached all facets. Certainly we have OPSEC plans, certainly we talk to people before they go on travel, certainly we look at travel orders, certainly we have it in our exercises for mobility, but we still have two areas of chief concern where quite frankly we haven't done as good a job as we'd like to. The first area is in computer security. Yes, we've worked very hard to try and get good security going, but the problem is when you start talking about that elusive term of sensitivity the definitions and regulatory guidance are almost conflicting. In the computer area, you know the sensitivity when we are talking about classified information but when you talk about sensitive unclassified information we are talking about privacy data. We're talking about high dollar volume. Our chief problem has been with the stand alone word processor. A small example of that is where Mary Jane is sitting typing up a speech. It's on the word processor on a floppy disc. It goes for review and many things are considered sensitive and subsequently extracted from that presentation. But what's happened to it for the six months that it has been on the floppy disc. How are we going to protect that? Does it warrant protection? Remember, one of our first axioms is not everything warrants protection. The second area is how we deal with industry and quite frankly our office in general and probably me specifically have not done a very good job. The problem with that is that

unfortunately I'm in an arena, or in an area that there are still some feelings and I'm ashamed to admit it, but as soon as you say government and industry in some circles it's almost an adversary relationship. It's very similar to that adversary relationship that the atmosphere of mistrust that many have in government in general, especially in dealing with the public, and especially when dealing with the public in freedom of information requests. An example of that is one that passed through our office was that one such unsatisfied customer refused to believe, believe it or not, that the government only had records regarding the acquisition of the territory of Louisiana back to 1803 and persisting to know more, he finally got this response: Please be advised that the government of the United States acquired the territory of Louisiana by purchase from the government of France in the year 1803. The government of France acquired title by conquest from the government of Spain, the government of Spain acquired title by discovery by Christopher Columbus, an explorer, a resident of Genoa, Italy, who by agreement concerning the acquisition of title of any land he discovered traveled under the sponsorship and patronage of her Majesty the Queen of Spain. The Queen of Spain had received sanction of her title by consent of the Pope, a resident of Rome, Italy and ex-officio representative of Jesus Christ. Jesus Christ was the son and heir apparent of God. God made Louisiana. I trust this complies with your request.

In order for OPSEC to work, it must be ongoing and continuous and it has to be just as much of your overall security program as it is to lock your safe every night and the proper destruction of classified documents. It cannot be an on again off again, hit and miss proposition because under that system it will surely fail. Now, what we did, we sat back and did a little statistical analysis and I had a lot of my records prepared, but last night while most of you were out having fun, whether it was bowling, gambling, or going to a show, Bill Johnson and Dave Brown and myself sat down and did some statistical work. The first axiom that we came up with was figures don't lie but a lot of liars figure. You can get all the statistics in the world that you want but the bottom line is that 43 percent of all statistics are totally worthless. The next statistics I give you please don't ask me to defend, just trust me. We took five program

managers PMS within our activity and if you ask me for a hard reason why we picked this particular five I really couldn't give it to you other than they were there. The only semblance of order that they show is that we tried to pick some that were relatively new, some that were down the line three to five years, and some that were just about ready to be fielded. The problem with this information gathering and the problem of how we distributed information and how we protect it is this. We found in the protection of information and the exclusive holding of the information that in these particular five PMs, and I'm not trying to say that it works for the world, that the government held the information exclusively somewhere between five and 10 percent of the total time. What I'm saying in fact is that at Fort Monmouth, a particular PM gets a needs and requirement document. Many, many times their first step is to call a contractor to do an analysis. So what I guess I'm saying is, if we are using OPSEC to try and protect all this information and then we hand it over to industry and they don't have the same program with the same method, I think it's going to be tough to carry it through. As a personal opinion, I honestly believe that we have to be compatible and that an OPSEC program has to be ongoing in a facility or an installation and certainly for a particular contract it has to be modified, but the program in and of itself should be well implanted. Now you can all beat me up—any questions? Thank you very much.

GOVERNMENT SECURITY REQUIREMENTS—A THOUSAND FACES TO INDUSTRY

Irving T. Boker
United States General Accounting Office
Washington, D.C.

As you have observed in the program, my topic is "Government Security Requirements—A Thousand Faces to Industry." Don't Panic! I'm not going to cover all one thousand. Besides, a thousand may be a slight exaggeration. There's probably no more than 997.

Let me make one thing clear. Neither I nor the general accounting office would expect the

Department of Defense or any other large government agency to establish security rules for industry that could be applied across the board without exception. There is just too much going on to expect that. There are some situations that require exceptional treatment. However, when the exceptions become a way of life, to the extent that many such exceptions are not justified on the basis of need versus cost, then we have a problem. As a matter of fact, we have many problems. I want to discuss some of these problems with you, such as OPSEC, TEMPEST, and Carve-outs. My primary purpose is to encourage you to question the need for some of these special requirements. I don't expect you to buck the system, not if you need your job. On the other hand, docile acceptance of any and all special requirements is not good for security, not good for the government, and generally not good for industry.

Perhaps a little background of how we arrived at where we are today would be helpful to a better understanding of DoD's Industrial Security Program. I'm only going to cover some of the highlights.

In 1955, Congress established the Commission on Government Security "to fill an urgent need for an objective, nonpolitical and independent study of the innumerable laws, executive orders, regulations, programs, practices, and procedures intended for the protection of the national security; to establish fair, uniform, effective, and realistic measures to safeguard both the national security and the rights of individuals; to obtain the greatest practical uniformity; and to restore full public confidence in the government's program to protect the national security." The Commission became known as the Wright Commission, named after its chairman, Lloyd Wright. In June 1957, the Commission issued its 800 page report to the President and the Congress. The report covered a wide range of topics related to national security—document classification, personnel security clearances, and industrial security, just to name a few.

The Commission made several recommendations involving industrial security. Perhaps, the most significant of these was the Commission's recommendation that an Office of Security be established within the Office of the Secretary of Defense to insure uniformity within the military

services with respect to DoD's Industrial Security Program. As might be expected, the military services were reluctant to relinquish their responsibility for the security of programs involving industry. Their reluctance is understandable. After all, the Army and the Navy had been responsible for their own information security programs inhouse and in industry since, at least, World War I. You might compare their reluctance to your reluctance in delegating the running of your household to your mother-in-law.

Even before the Wright Commission, in the late '40s, DoD was concerned about the lack of uniformity in requirements and lack of reciprocity among the three services. Not only did contractor employees have to be granted clearances by each of the services, sometimes they had to be cleared by various bureaus within each service. DoD conducted various studies and major improvements in the Industrial Security Program were made. For example, the Armed Forces Industrial Security Regulations were issued in 1953. In July 1965, the Secretary of Defense issued the directive which is the basis for today's Industrial Security Program. According to the directive, the Office of the Secretary of Defense would provide overall policy guidance. The responsibility for security cognizance or administration of industrial facilities was given to the Director of the Defense Supply Agency, which later became the Defense Logistics Agency. In October 1980, the group within the Defense Logistics Agency, which had responsibility for Industrial Security Administration, was transferred to the Defense Investigative Service where it is today. At least, it was when we left Washington.

As you know, an Industrial Security Manual, containing uniform security practices, has been issued to contractors for many years. Now, if this 344 page manual and classification guide were all that most contractors needed to follow to satisfy the security requirements of a classified contract, and if DoD components generally required no more than what was included in the two documents, I could stop talking. However, we have not arrived at Camelot yet and, from all indications, we are proceeding in the opposite direction at an ever increasing pace. I'm going to briefly discuss three areas where we have identified major inconsistencies—OPSEC, TEMPEST, and carve-outs.

OPSEC, Operations Security, is one of the more recent developments affecting industry, but OPSEC is not new to DoD. In October 1974, the Joint Chiefs of Staff issued Publication 18 on OPSEC, and in 1975, the military services started issuing implementing regulations. Publication 18 and the implementing regulations, however, are directed primarily to military operations. As far as we could tell, prior to 1981, few industrial facilities were required to implement OPSEC measures. As more contractors were required to incorporate OPSEC at their facilities, their complaints about the costs and need for OPSEC measures also increased. Consequently, DoD issued a new OPSEC directive in July 1983, which identifies, in more detail than previous DoD instructions, the responsibilities of the military services and other components, with respect to OPSEC in industry. The directive states that it is DoD's policy for each component to establish an OPSEC program. Now, that may be alright with respect to internal operations, but it could be the beginning of chaos when applied to industry. There have been coordinating meetings among representatives of the Defense Investigative Service and the components, but if this program is typical of past performance, despite the best of intentions, industry can expect a myriad of inconsistent OPSEC requirements in the future.

Several months ago, we completed a survey of OPSEC in industry. Perhaps, we were a little premature in starting a review; nevertheless, we noted a number of inconsistencies, starting with the OPSEC plans. One of the basic features of the OPSEC program is preparation of an OPSEC plan. It's similar to the standard practice procedures that are required before a facility security clearance is issued. In some cases, the DoD components provided the plans to the contractors, in the form of appendices to the classification guides. In many cases, the contractors were required to prepare the plans. Preparation of the plans was a problem for some contractors because they were in no position to identify the hostile intelligence threat—the basic foundation of the plan—and the components had not furnished the information. Our guess is that the components, themselves, may not have had complete knowledge of the hostile threat in the geographic areas where some of the contractors were located.

In addition to identification of the hostile intelligence threat, OPSEC plans contain three other

basic sections—identification of the sensitive aspects of the contract, assessment of the vulnerable areas of operation, and proposed countermeasures. Let's talk about countermeasures, since they involve a continuing effort by contractors. We identified about 20 types of countermeasures in the 14 OPSEC plans that we reviewed. Of course, the need for specific types of countermeasures will vary among contractors, depending on the program and their particular involvement. However, certain basic types of countermeasures would appear to be desirable, regardless of the program or contractor. We found many inconsistencies in the application of basic types of countermeasures. For example, only about half of the plans required the contractors to assure the security of conference rooms where classified information was discussed. I suspect that, if we were to make a review a year from now, the situation would be worse than it was several months ago. I hope that I'm wrong.

Another item of concern are the OPSEC inspections. According to the DoD directive, the Defense Investigative Service has primary responsibility for conducting OPSEC inspections, but components are authorized to make some inspections, after coordinating with the Defense Investigative Service. We found that one component was making OPSEC inspections, which were in addition to the semi-annual inspections by the Defense Investigative Service. We've been assured by DoD that the need for a uniform OPSEC policy for industry and inspection responsibility were being resolved.

For those of you new to security, TEMPEST is not a sand storm here in the desert nor a wind storm in Washington. TEMPEST, according to the official government definition, is an unclassified name that refers to the investigation and study of compromising emanations. Compromising emanations are signals from information processing systems, which, if intercepted or analyzed, could disclose national security information. Until a few months ago, I had always thought of TEMPEST in relation to protecting Sensitive Compartmented Information (SCI). Then, I learned that TEMPEST was not confined to SCI. My initial reaction was, man, are you ignorant! Then I looked at the Industrial Security Manual, and found that I was not alone in my ignorance. I couldn't find any mention of TEMPEST, not the word itself nor

a reference to it, even though a 22-page section of the manual was devoted to Security Requirements for ADP Systems, including Word Processing Systems. These requirements are for the protection of classified information, TOP SECRET, SECRET, and CONFIDENTIAL.

Last year, we received a call from a contractor who told us that one of the military services was requiring the contractor to establish TEMPEST control measures for SECRET and CONFIDENTIAL information that was being processed. In this case, the Security Manager thought that the TEMPEST measures were unnecessary because of the low volume of classified data being processed, and because neither the CIA nor NSA was requiring any upgrading of protection for the Data Processing Operations. Unnecessary costs, that is, the cost of control measures would have been about five hundred thousand dollars. In case you're wondering how this case turned out, most of the anticipated costs were avoided, thanks to the security manager raising the question of need for TEMPEST control measures.

I can assure you that this example is not an isolated case. We know of several similar cases. Now, another question a person might ask is, how does something like this happen? Apparently, these cases occurred because of a change to the Armed Services Procurement Regulations in February 1983. Defense Acquisition Change #76-42 stated that, "Whenever ADP equipment or services are acquired which are to be used to process, transmit, store, retrieve or display classified information, the contracting officer shall insure that the equipment involved in the acquisition has been certified to meet minimum standards to protect the classified information from possible compromise due to electronic emanation." It seems that some well-meaning, but ill-informed, individuals in one of the military services took this requirement literally, and even expanded it. I guess, by extrapolation, you could reason that, if you have TEMPEST approved equipment from the preferred products list, you should house it in a facility that meets TEMPEST requirements. Makes sense, doesn't it? Yes, except for two things. First, the cost of facility protection, such as lead shielding, generally, is substantially more expensive than equipment protection. Second, some consideration should be given to the frequency or volume of classified information

being processed, its level of classification, and the potential threat or risk of compromise, compared to the estimated cost of protection. In several cases that we know of, this was not done until the contractors complained of the need for TEMPEST requirements and requested direct reimbursement for costs that would be incurred. What are we talking about, with respect to classified information and cost. Well, less than 10 percent of the information being processed was classified and most of that was classified CONFIDENTIAL. The estimated costs of TEMPEST protective measures for the contracts ranged from \$100,000 to several million dollars. Strangely enough, these horror stories were confined to one military service, one where almost everything related to security is delegated down the chain of command and there is little internal control.

Last September, a TEMPEST Committee from industry completed a survey of aerospace contractors. The Committee concluded that while there was TEMPEST vulnerability, there was no evidence of threat exploitation. Consequently, the threat was minimal, compared to the countermeasures being imposed, which were costly and disproportionate. The Committee also found that there was little consistency among the agencies requiring TEMPEST measures and an inconsistent application of requirements by a customer to different contractors.

In all fairness to DoD and the intelligence community, an instruction was issued a few months ago that identifies the criteria to be used in determining whether TEMPEST measures are needed. However, the instruction is classified and is not available to contractors. It might be helpful to contractors if the ADP section of the Industrial Security Manual contained some TEMPEST guidance.

At these seminars, there always are a number of attendees who are new to security or who have not been exposed to carve-outs. For their benefit, a quick definition. A carve out or carve-out contract is a contract for which the Defense Investigative Service has been relieved of responsibility for security administration. Essentially, that means that the military service or DoD component that awarded the contract will make, or it is assumed will make, periodic security inspections. The rea-

son why I stressed "assumed" is because, we found some cases where the military services had not inspected contractor facilities for 4 to 6 years, to verify that sensitive documents were accounted for. And representatives of the Defense Investigative Service, during their semi-annual inspections were not allowed to review records of individuals who had access to carve-out contract data or to determine that all the data that the contractor was supposed to have was accounted for.

There are two major types of carve-out contracts. Those that involve SCI and those that do not. For the few of you who may not know what SCI is, it is intelligence or intelligence-related information. Standard procedures have been established for contractor handling of SCI, but they are minimum standards, and often are exceeded at the direction of DoD customers. Unfortunately, not even minimum standards have been established for the special handling of non-SCI, or collateral information.

You may be wondering what these non-SCI contracts are for. They may be for a wide range of activities, from research on exotic new weapons, special studies, technical support for very sensitive, complex existing systems, they might even be for the construction of a golf course. I'm only joking; we haven't found any of those --yet. Nevertheless, sometimes, carve-outs are used to expedite procurements and to make sole source awards, circumventing the competitive procurement process. Although, according to DoD regulations, carve-out contracts are to be used only in support of approved special access programs, it is doubtful that all carve-outs do, in fact, support special access programs. But even the number of authorized special access programs has grown. In 1979, DoD had 10 official special access programs. In 1982, there were 50 currently, DoD has over 100 special programs. Some of the increase is attributable to better reporting of such programs by DoD components to the office of the Secretary of Defense. Improved reporting is the result of revisions to DoD's information security program regulation in August 1982. However, a good part of the increase is due to more programs being established. We understand that the majority of these 100 odd special access programs are non-SCI programs. Odd is a good word to describe some of these non-SCI special pro-

grams because, if they are supported by contracts, you can bet that they are odd in that security requirements for contractors will vary greatly. The number of carve-out contracts is also constantly growing, but I don't believe anyone knows the exact number, or even a close approximation. We guess, and I don't say estimate, because that would imply some degree of precision and that certainly is not the case. We guess, conservatively, that there probably are about ten thousand carve-out contracts. But, what does that mean, as far as security requirements are concerned?

In case you haven't noticed, I only ask questions that I can answer. The explosion of carve-out contracts means that industry is faced with a multitude of special, duplicative, sometimes inconsistent, sometimes unnecessary, but almost always costly security requirements. Most carve-out contracts require special access listings of the individuals authorized access to the contracts, based on a need to know. Here again, my ignorance shows. I have always thought that "need to know" was the basic rule for access to any classified information. Is DoD implying that government and contractor employees with security clearances can't protect classified information unless it is carved-out? I have always thought that the designation of "TOP SECRET" was intended to protect the most sensitive information. Why isn't TOP SECRET used more often? The information in many of these carve-out contracts was only classified at the SECRET level. During our review of carve-outs, which was completed in February 1983, we were told that about 39,000 contractor employees had been given special access authorization to non-SCI contracts. Of the 39,000, almost 14,000 had security clearances at the SECRET level. In addition, about 12,000 contractor employees had been granted SCI access. One DoD official thought that the number of contractor employees with special access to both SCI and non-SCI contracts, was probably in the neighborhood of 150,000. Inasmuch as DoD had good centralized control over SCI accesses, but not over the non-SCI special accesses, we could assume that anywhere from 39,000 to 138,000 contractor employees had non-SCI special accesses. Perhaps, as many as a third of those, or about 46,000 individuals only had SECRET clearances, even though they were involved with contracts that had been considered too sensitive to be a part of the mainstream of the Industrial

Security Program. If you are familiar with security clearance procedures, you know that a SECRET clearance can be granted to a contractor employee on the basis of a favorable national agency check. A TOP SECRET clearance must be preceded by a favorable background investigation and an SCI access must be preceded by a favorable special background investigation which is more extensive than a regular background investigation.

Paradoxically, some of our most serious compromises of classified information have involved carve-out contracts. Are the added security costs associated with carve-outs really effective, or would there have been more compromises without them. I don't think we'll ever know. We do know that physical security is expensive and where carve-outs are involved, generally, it is much more expensive. Data pertaining to SCI and many non-SCI carve-out contracts is maintained in sensitive compartmented information facilities. The size of these facilities can range from one room, comprising 120 square feet, to a complex of rooms totaling 40,000 square feet, even whole buildings. The cost of these facilities can run from about \$15,000 to about \$5,000,000. We understand that the average cost is about \$125 a square foot. These facilities, either a room or a complex of rooms, resemble a bank vault. The protective devices include combination locks for the doors, alarm systems of the usual variety, intrusion sensors, approved containers or safes with combination locks, and sometimes, even an alarm system for the safes. One place that we visited had three sets of doors with combination locks that you had to go through to get into the compartmented facility and three alarm systems including one on the locked containers. If we have established the standards for protecting CONFIDENTIAL, SECRET and TOP SECRET information, are these other measures absolutely necessary? The application of these other measures is so inconsistent and costly that it defies imagination. The name of the TV show, *That's Incredible*, would be an appropriate description of the security requirements placed on industry.

In conclusion, when I'm in the audience, those are two words that sound like a wake-up call. I have only touched on three areas of inconsistent and costly security requirements. Last September, one of our NCMS members, Junius Layson, was a member of a panel on government security

at the Annual Seminar of the American Society for Industrial Security. And he assembled an excellent presentation of the many contradictory security requirements that have eroded the one face to industry concept. I'm sure that if you asked him, he would give you a copy.

Let me close with my usual, slightly modified quotation from Abraham Lincoln. "We have always wanted to deal with everyone we meet candidly and honestly. If we have made any assertion not warranted by facts, and it is pointed out to us, we will withdraw it cheerfully."

SECURITY RESPONSIBILITIES FOR MANAGERS

James Mood
National Security Agency
Washington, D.C.

Good Morning Ladies and Gentlemen. It's true that I am going to digress a bit from the Technology Transfer theme. In doing that I would like to explain . . . but first may I ask how many of you are security managers; that is, you supervise a number of security people in a security department or organization? That's about 75%, thank you! How many are managers in a field other than security? Another 5 to 10%. Now, how many of you are not managers, but work in a security organization in Government or industry? Another 5 to 10%, thank you! I now know who you are—and that's important!

The reason I asked is because I want to discuss security responsibilities for managers—not just security managers, but managers or supervisors in general. And, what I want to talk about is a classic area of human behavior, "the psychological aspects of reporting."

Yesterday Maynard Anderson, in his keynote address, talked about the technology transfer problem. He repeatedly made reference to the Soviet threat and the "Soviet empire" as the main recipient of stolen high technology from the West. Later, in his talk, Tom O'Brier stated that one of the key ways to counter the loss of high technology was through education and awareness . . . making the marketeers, the engineers, and the

technicians aware of the laws, prohibitions and concerns regarding the export of such items.

Although I am not an expert on technology transfer, I believe that one of the most effective ways to counter the loss of high technology (or sensitive or classified information in general) is to understand the attitudes and behavior of people when they become aware of a particular problem, and to help those same people recognize this behavior in themselves so they can better deal with it. I believe that everyone in this room will, to some extent, be able to identify with this problem, and with the psychological battle each of us must fight within ourselves when we are confronted with the decision to report someone.

Let me begin by sharing with you a true story. It happened to a friend last summer, in Ocean City, Maryland. It was a warm September weekend and the beach was crowded. The group of people my friend was with were near the water's edge when—all of a sudden—a woman came out of the surf screaming for help, and pointed to two men in obvious trouble beyond the breakers in deep water. It was apparent that they would drown if they didn't get some help quickly. And, just as apparent, the woman was pleading directly to my friend for help . . . and everyone in the area, including his family, were expecting him to make a galant dash into the surf and rescue the swimmers. So that's exactly what he did! And, as he swam toward the troubled men, thoughts came to his mind that he neither expected nor liked.

Keep in mind the circumstances. The beach is crowded and all eyes are on him. Everyone is expecting him to do the *right* thing. But, what about these thoughts? He's beginning to rationalize, to have second thoughts about this "hero stuff." First of all, he realizes that there are two of them and only one of him . . . and that both of them look "bigger and stronger" than he. Second, he remembers that in his rush to the surf he forgot to grab something to throw to them—no raft or tube, not even a towel or belt. Finally, when he is close enough to see the panic in their eyes, he realizes that he is "surely going to die"; he will be pulled down with them. Now all he wants to do is turn around! Why should he sacrifice his life? They're finished anyway . . . there's no way he can change that . . . so why not turn around? If he doesn't "he only has a couple of minutes left." It would be wrong *not* to turn around!

I've gone on long enough! I said this was a true story and it is. It ended when my friend "the hero" finally reached the swimmers. Instead of being alone, he suddenly discovered that fifteen or so others had heard the woman's screams and arrived on the scene at the exact moment he did! Although we have a "happy ending" to our story, what about our hero. If he didn't have his family, friends and hundreds of others watching his every move, what would he have done? Would he have let two men drown? Did he sufficiently rationalize in his own mind that the "right" thing to do was turn around and swim back to shore and safety? Is my friend a coward—or is he normal? I'm not really sure, but I'll confess to you that the friend, the hero or the coward, was in fact me!

I believe all of us, to some degree or another, go through a similar rationalization process whenever we are confronted with a difficult decision, or an action that we don't really want to face. Can you relate to that? And for our purposes today, the decision or action I'm concerned with is "recognizing and reporting" a serious problem about someone to appropriate officials in your company or agency. The problem of a friend, a co-worker, or a supervisor. The problem may concern security, mental or emotional stability, drugs or alcohol, or any number of other areas. Don't kid yourself, for most of us the decision to report a friend or co-worker could be one of the most difficult we face throughout our entire life. And, like that swimmer, right and wrong decisions become jaded when other considerations, fears and emotions get involved.

It is my opinion, based on twenty years experience, that only a small percentage of the serious problems identified by people are actually reported to appropriate officials. I base this on "after-the-fact" investigation. In case, after case, after case, we find that serious indicators of major problems were known by others—co-workers, friends or family—but were *not* reported. Not just in security matters, but in technology transfer cases, suicides, drugs, theft . . . and I could go on and on! Let's try to examine some of the reasons why. . . .

First when we talk about identifying a problem; it is a matter of opinion . . . of one's point of view. A person who drinks three beers a day might be considered a heavy drinker to a non-drinker—and a "teetotaler" to a heavy drinker. Most of us

struggle to own a home and pay our bills. Some, however, may consider that irresponsible and serious indebtedness. Asking questions on the job and staying after hours may be seen by some as conscientiousness, but to others the individual is nozy, suspicious and violating the need-to-know. Thus, the first point I want to make is that you as managers have to identify as clearly as possible to your workforce what you would like reported!

I talked to a lady where I work two weeks ago who said that she had been there 18 years, and during that entire period she had never seen one problem that would require reporting. In my opinion, she saw the problems; she just didn't recognize them. She didn't know what to look for! People everywhere have problems! People with sensitive jobs and clearances are no different from everyone else.

Secondly, you must try to convince your employees that reporting someone is *good*—that it is the right thing to do! Not because the security officer says it is—but because *you know it is!* Therefore, you must try to counter or reverse the negative connotation attached to reporting someone.

When was the last time you heard someone say it's a good thing to report someone. What is it about our society and our country that tells us that when someone may be doing something to harm it, you are a "rat fink" if you report it? Isn't that the mentality we all live under? When we were little kids what did our mom and dad teach us? Don't be a tattletale!

"If you can't say something nice, don't say anything at all." We were taught not to say things about people that aren't nice. All kinds of nasty nicknames go with reporting someone. Even people in security or police work talk about finking on somebody or ratting on somebody. It's got a negative connotation that's hard to shake. You have got to try to reason with your employees to counter such thinking. Point out the positive results!

The next problem that we have to recognize is the problem of "fear." This is the one, in my opinion, that we have to lock inside ourselves to deal with. We all have fears! Fears are what shape our personality; fears are what shape our lives,

our decisions and our careers. Fears are what keep you from going out in that Casino and betting your life savings.

Let's look at some of the fears that many of us have when we see something that should be reported, or when we see something that we think might be wrong. The first fear is that we're afraid that we might be wrong about what we see or think! Now if you see someone in your office with a brown bag with the strong smell of liquor, and about every five minutes the individual is sipping whatever is in that bag, then I would say you can conclude with some assurance that that person has a drinking problem.

But, most problems are not that obvious. Usually when you see something you've only got suspicions, you've got gut feelings, sometimes you've got meaningful evidence, but even then most people will not make a report unless they have the facts. Let me tell you that you will almost never get the facts! That's for the people who receive your report to determine. That's what they're paid to do—let them do their job!

Still another fear is what the people will think when we report the information. Will they share our concern, or will they think it's ridiculous! Remember, right and wrong is sort of in the eye of the beholder! Morality is in the eye of the beholder, a drinking problem is in the eye of the beholder. So what you may think is a problem based on your upbringing and your knowledge may not be shared by someone else. So you may have a fear about whether or not they're going to agree with you; that it might not be looked upon as a serious problem.

What's an even bigger fear? Can someone help me? How about being afraid that people might become aware of you—the *person who reported the information!* Your co-workers might find out, or worse, the source of the accusation or allegation! Now that is *real* fear, isn't it? Finally, one of the most frequently experienced fears is the fear that the people you report the information to will not handle the problem properly. This, more appropriately, might be a lack of confidence in the organization (in your agency or your company) where it's the security department, the medical center, your senior managers or your immediate bosses. You lack the confidence in the

people that you have to report to that they will handle the problem the way you think it ought to be handled! I could go on and on identifying fears; all of us have them and they become a major factor for many of us when we consider reporting someone.

Another factor that can often be a detriment to reporting something or someone is loyalty. Loyalty is an interesting phenomenon because we are often not aware of it. Sometimes we do not understand what influences us to side with one person over another, or take a position in favor of one or another . . . but frequently the reason is not the issue we are supporting but loyalty to that person or the issue. Let me illustrate my point by sharing a personal experience. As a manager of supermarket cashiers (checkers) for four years while in college some twenty years ago, there was a continuous problem of checkers estimating the price of certain daily staples such as milk and bread. Estimating took place because these items were never marked and prices changed frequently . . . sometimes daily. It was a known fact that a checker almost always estimated in favor of the store rather than the customer. In fact, when a checker made an error, 95% of the time it was in the store's favor . . . even when the checker was disgruntled in his/her job or angry at the employer. The reason was a subconscious loyalty.

Although there is no question about our loyalty to our country, we have other loyalties too . . . to our employers, our co-workers, to causes we support; loyalties that we don't think about and, sometimes, are not even aware of.

Let's look at some of the feelings or the rationalizations that people have to deal with in this area . . . when someone you know; a co-worker or a peer has a problem. First of all there's a subconscious dislike in all of us for the bureaucracy . . . the establishment, the big, impersonal system. It doesn't matter whether it's General Motors or the Department of Defense, the "system" is *there* and we're here . . . most of us do not consider ourselves part of that big powerful system. We're in it, but we're individuals; we're a little different than the rest. Carrying this thinking one step further, we often rationalize: "Why should I report my friend or my co-worker?" We are down here at the working level and my co-

worker's got a little problem; but management has seen the problem for years so why should I be the one to report it? Besides if they wanted to do something about it they would have done it by now! They're the guys that make all the bucks, let them earn their money!

How often have you heard rationalization like that? Or, how about some of these comments . . . They created "the system," they promoted who they wanted to promote, they see what they want to see and they ignore what they want to ignore. Why should I stick my neck out to turn in my friend? He's my friend, he's a hard working guy, he's a good family man and a good provider. So he's got this problem. It doesn't have any effect on his clearance. He's never done anything wrong that I've seen and he's a little guy like me. No matter what he has done, I'm not going to place my friend at the mercy of the system, to risk his clearance and his job, would be unthinkable. Now I'm not saying that this kind of thought process is going to be obvious to you, but what I am saying is—whether you like it or not—you're going to go through a personal struggle and are going to rationalize, and it may not be an exercise that is obvious to you.

Now let's discuss a couple of other factors. Do you remember taking the old multiple choice tests in high school or college? What did the teachers tell us to do when we took those tests? If you're not sure of an answer, put the check next to the one that comes to mind first! Right? When you go back and change a multiple choice question, it's been statistically proven that the likelihood is that you're going to go with the incorrect answer! The same thing is often true about people, if you have a "gut" feeling that there is a problem and you consider yourself, or your friends consider you a person with a reasonable amount of common sense and judgment (and you think there might be a problem) ladies and gentlemen, most likely there is a problem! So as I said before, don't wait until you have all the facts because that probably will never happen.

Secondly, you the co-worker, the immediate supervisor, or the friend are very likely to identify this problem before the security department or the medical center. You work with the person; see him every day! Senior management doesn't; they're not going to know the problem exists! If

someone commits a crime, someone deliberately violates a security regulation, someone is doing something they shouldn't with sensitive material; you're the one that's going to see it!

Third, while you may have concern, and many times it's a very legitimate concern, over the proper handling or resolution of an issue, you must not allow that concern to keep you from fulfilling your responsibility. The people in the area that you have supervisory control over; if they know something and they work for a contractor, or department or agency of the government, they have a responsibility to report it.

And fourth, if you do have questions that remain unanswered, if you have concerns; the way to resolve those concerns is by meeting privately with the individuals you are responsible to in this particular problem area. Whether it's the security people, your boss, or whatever; talk to them and try to resolve it.

Now, let me quickly review some of the kinds of problems that need to be reported. Again, these are applicable to the technology transfer problem, just as they are to security and other concerns. Technology transfer and espionage are often the same kind of problem as far as I'm concerned. I saw an article in the *New York Times* within the past month and the headline in the article was, "Chinese involved in stealing Western high technology." When you read the article you find that Chinese diplomats have been stealing high technology from the U.S. government. We used to call that espionage! You can call it technology transfer or espionage, whatever it is the end result is the same, isn't it? Let's just look for a minute, and again, I'm not a psychiatrist or psychologist, but these are common sense indicators of problems, and what I'm doing is putting most of them together in one list for you to think about. A first concern would have to be any extreme or sudden change in an individual's personality or behavior pattern. Some examples are: severe depression or a sudden change in job performance. If you've got somebody that is your absolutely top drawer employee and suddenly he becomes a really sleazy employee you better be looking to see what's causing that change. Conversely, if you've got a really lousy employee and that employee has been a jerk his entire working career and suddenly he becomes a super

employee, you had better look into that change also. Look at any type of erratic behavior or any serious emotional problem. What's a serious emotional problem? I don't know, but again I think that most of us would recognize serious emotional problems when we're confronted with them. When you work with someone day in and day out you become pretty close to them and I think these things become pretty visible when they occur.

From the security aspect, any deliberate violation of government security regulations or company security regulations, that involve the control and protection of either sensitive or classified information or high technology. If there's a deliberate violation, regardless of the excuse, you better let someone know about it! Any improper handling of sensitive or classified information to include taking material home (if it's against company regulations) obviously it is if it's classified!

Any suspicious or unreported contacts with foreign nationals. What's a suspicious contact with a foreign national when you live in some place like San Francisco? I don't know folks! I would say that if you've got an individual that has close associations with citizens of a communist or communist controlled country and that person has a clearance, you have a potential problem there that should be looked at.

If you have an employee traveling consistently to a certain area of the world, and that travel is neither consistent with his or her financial situation, interests, or their job, you have a potential problem there. You better let somebody know about it! Also, any travel to denied areas for those of you with the clearances at the higher levels, without approval would be something that you definitely would want to report.

Report any open expressions of discontent, disloyalty or dissatisfaction with our country or our democratic way of life. I'm not talking about complaining about high taxes or the national debt, or the reduction of benefits or whatever your gripes are. Again, you should be able to recognize the difference!

If an individual obviously is suffering from excessive indebtedness or sudden unexplained affluence—that deserves the prompt attention of

someone and it should be resolved; not necessarily by security people, but it should be resolved!

If you have an employee that's been involved in a serious crime, again as a co-worker or a friend, you are going to know about that before senior management will. Report it!

And finally, anyone whose activities or conduct violates the need to know such as working overtime or after hours and visiting other work areas for no apparent reasons. Someone better look into that individual's activities and make sure they're valid.

Let me conclude very, very briefly. If you recognize that reporting potentially adverse information about someone is an extremely difficult decision making process, then you may also admit that we often mull over such a decision for months. *You are ahead of the game!* Just recognizing the problem is the first step. Secondly, remember that there are laws that protect you, protect your identity, and protect the information you provide and your right of confidentiality. That should be a positive part of your deliberations to make a report. You can be protected, and anything that would lead to your identity would be protected. Thirdly, allegations against someone are never accepted at face value if they are reported to the proper authorities. They are resolved through careful investigation and careful deliberation. The rights of the accused individual are always a first consideration. I have confidence in the companies that are represented in this room as well as the U.S. Government departments and agencies. I can tell you that the rights of the individual today are protected very, very well. Finally, common sense and good judgment are all that is necessary in assessing the seriousness of a matter, and in deciding whether or not to report it. It is best not to seek someone else's advice in such matters. What you're in effect doing is compromising your own feelings and your own opinions, for the judgment of someone else. You will never end up getting a problem resolved that way. If you need to discuss it with somebody, take it to your management or take it to your security office! Thank you very much!

TECHNOLOGY TRANSFER DEVELOPMENTS AT THE OSD LEVEL

Anthony G. Mitchell
Deputy Director, Information Security and
Special Programs
and
Mr. David E. Whitman
Directorate of Security Plans and
Programs
Office of the Deputy Under Secretary of
Defense (Policy)
Department of Defense
Washington, D.C.

I will speak to you this morning concerning some of the Defense Department's current activities designed to control technology transfer. They will include:

- The 1984 Defense Authorization Act and its withholding authority;
- Our implementation of that Act, its status, responsibilities and future;
- The distribution limitation statements on technical documents and their flexible revisions;
- Our foreign disclosure and technical information system; and
- The militarily critical technologies list (MCTL).

All of these activities are designed to control the disclosure of militarily critical technology and to prevent handing our technical advances to the Soviet Union on a silver platter.

Our intent is not to create a monolithic, resource-draining bureaucracy to stop the flow, but to create, at modest cost, some devices that will preserve our informational advantage by controlling the disclosure of sensitive national security related technology while preserving the competitive position of American industry in the world market. And perhaps, as a salutary side effect, stop contributing to the creation of a generation of lazy Soviet scientists.

Many initiatives are ongoing and my remarks are not intended to cover all Office of the Secretary of Defense (OSD) actions.

The 1984 Defense Authorization Act gave the Secretary of Defense authority to withhold from public disclosure any technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be exported without an approval, authorization, or license under the Export Administration Act or the Arms Export Control Act. Technical data may not be withheld if state or commerce regulations authorize export pursuant to a general unrestricted license or exemption in their regulations.

- The new authority closes a loophole in the export laws stemming from the Freedom of Information Act (FOIA). Export laws (in effect) conserve U.S. technology while FOIA tended to force DoD to give it up upon request. Once information is made public effective application of export control laws is not possible. Although David S. Brown, Professor of Management, School of Public Administration, George Washington University, says "The greatest contribution to openness in governmental administration is not the Freedom of Information Act—but the xerox".
- DoD published its proposed implementation in the Federal Register for public comment in December of last year, we received about 80 sets of well taken comments pointing out room for improvement which has been done, final product will allay most if not all concerns raised.
- In early April a revised draft, based on the comments received, was sent to all those who had expressed interest for their further consideration. It was also sent on an informal basis to several interested committees on Capitol Hill for their reaction. A second round of internal DoD coordination was also undertaken in early April of this year. Replies were due back in early May. Final adjustments will be made and after that the proposed implementing directive goes to the Senate and House Committees on Armed Services and appropriations for their review prior to implementation.
- DoD implementation will not stifle scientific innovation necessary for continued U.S. advancement of the technological state-of-the-art but will slow down the unintended export of U.S. technology to adversary nations.

- Full implementation is more than half a year away.

The current proposal (DoD Directive 5400.XX—"Withholding of unclassified technical data from public disclosure) to implement the new SECDEF authority looks like this:

- It does not affect the dissemination by a private person of technical data developed without DoD funding even if the department is in possession of such data.
- It does not introduce additional controls on technical data already in the possession of DoD contractors beyond those specified by export control laws or in contracts.
- It does not introduce controls on dissemination of scientific, educational, or other data which qualify for general license GTDA under the export administration regulations.
- It does not change DoD responsibilities to protect proprietary data of a private party in which DoD has "limited rights."
- It does not affect release of technical data by DoD to foreign governments pursuant to official agreements—licenses—or arrangements with the U.S. Government.
- It does not apply to classified technical data.

Central to the technical data control mechanism is the concept of establishing a large pool of "qualified U.S. contractors" that may be private individuals or enterprises who would certify:

- That the person who will receive export-controlled technical data is a U.S. citizen.
- That the data will be used in connection with a legitimate business that is described in the certification—this does not require a contract or grant from the U.S. Government.
- That responsibilities under export control laws are understood and will be observed—this includes recognition that release of technical data within the United States with the knowledge or intent that it will be transmitted to a foreign country is illegal.
- That the business will not provide access to the data to other than its employees except as allowed by the proposed directive.
- That no person who will have access is

- debarred or violated export control laws.
- The contractor itself is not debarred and has not violated export control laws.

Canadian contractors may also be qualified under the draft for most technical data with an equivalent certification.

Because public disclosure of technical data subject to the draft directive is tantamount to providing foreign access—withholding such data unless approved—authorized or licensed in accordance with export laws is necessary in the national interest.

Technical data within the scope of their certifications would not be withheld from “qualified U.S. contractors” but would be withheld from others based on the controlling DoD office’s finding that:

- Such data would require a license for export.
- A general unrestricted license or exemption does not apply.
- The technical data have significant military or space application as indicated by the Militarily Critical Technologies List (MCTL).

The controlling DoD office is to assure that technical data subject to the draft directive are marked with the proper distribution limitation statement from DoD Directive 5200.20—“Distribution Statements on Technical Documents.”

Qualified U.S. contractors may disseminate technical data governed by the directive without prior permission of the DoD component where such dissemination is:

- To any recipient for which the data are licensed.
- To existing or potential subcontractors who are also qualified U.S. contractors within the scope of their certification.
- To the state or commerce departments for application for a export license—such applications are to be accompanied by a statement to the effect that the data are governed by the new directive.
- To the congress or other governmental agencies.

The office of the Under Secretary of Defense (Research and Engineering) will be charged with most of the responsibilities under the new directive including the development of procedures to collect and disseminate certification statements. Right now it appears that the Defense Technical Information Center (DTIC) will be at the center of this process and will even install a toll-free 800 phone line to facilitate answering the basic question about who is qualified.

Implementation of the directive will be phased in to allow for the establishment of a large pool (100,000 is possible—even probable) of qualified U.S. contractors.

DoD Directive 5200.20—“Distribution Statements on Technical Documents” has been around for a long time and provides for application of one of two distribution statements—“A” or “B”—on DoD technical documents:

- Statement “A” means a document so marked is “approved for public release—distribution is unlimited.”
- Statement “B” means distribution of a document so marked is “limited to U.S. Government agencies only” and other requests for the document have to be referred to the controlling DoD office.
- We suspect that this system of marking technical documents may have contributed to the unintended export of U.S. technology.
- If the originator of such a document marked it “A”—then it was assured that everyone who wanted to have it would be able to get it without any further administrative action.
- If marked “B”—only those in the U.S. Government could get the document through DTIC. DTIC had to refer other requests to the originator and special arrangements had to be made to get the document to industry. Both aspects of this situation meant more work on the part of the controlling DoD office and more red tape that was self-imposed.

Recognizing the need to provide more flexibility in the marking system the Secretary of Defense, on 18 October 1983, issued an interim policy that effectively revised DoD Directive 5200.20 to provide for a total of 6 markings as follows:

- "A" and "B" remain as before as mentioned above.
- Statement "C" means "distribution limited to U.S. Government agencies and their contractors."
- Statement "D" means "distribution limited to DoD and DoD contractors only."
- Statement "E" means "distribution limited to DoD components only."
- Statement "F" means "further dissemination only as directed by the controlling DoD office."

The new interim policy provides opportunity to be more selective in determining intended distribution patterns for DoD technical documents. Thoughtful consideration and use of these new distribution statements is intended to increase the sharing of unclassified DoD technology within our industrial and university community in order to make the best use of DoD resources. It is intended that the net effect of the new policy be a wider dissemination inside the defense community and a more selective dissemination outside the community of DoD generated information. In short, these new management tools should assist us to reach the intended audience.

Shortly after the interim distribution statement marking policy was promulgated General Stilwell (DUSD(P)) and Dr. Edith Martin (DUSD(R&AT)) reminded DoD components, as a practical matter, that technical documents marked with statement "A" are made available to the public and routinely receive dissemination outside the United States, either through U.S. Government programs or through private channels, and are readily available to countries which are hostile to the United States.

With this knowledge on the part of DoD technical document originators and the new distribution statement options, we may see less frequent application of statement "A" and fewer of our technical documents going straight to the Kremlin.

The Soviets consider the fruits of U.S. R&D programs to be their national resource—we are trying to dry up that resource in other ways.

The DUSD(P) has asked the PDUSD(R&E) to consider establishment of A Technology Screen-

ing Board at the Defense Technical Information Center. Agreement was reached rapidly and the Technology Screening Board should be functional before long. Detailed operating procedures are still being formulated but the new board will examine DoD originated technical documents earmarked as being available to the public (Statement "A") before DTIC sends them to Commerce's National Technical Information Service, and from there to the rest of the world. Questionable cases will be scrutinized and possibly made available to registered DTIC users only. Here again, the objective is to help assure dissemination to those within the defense community who have a need for the technical data:

- DTIC has been processing about 30,000 new acquisitions each year.
- About half of these have been statement "A" documents—a huge workload for the New Technology Screening Board.
- The number of statement "A" documents certainly will decline in the future as the new distribution statements are used but to what extent is not known.
- The new markings specified by the Secretary's Interim Policy are being used but not yet in large numbers. This is probably due to the pipeline effect. Many DoD technical documents take a long time to prepare and dissemination restrictions or their absence would have been considered at the outset. We will be watching the trends as one indicator of effective implementation of DoD Directive 5200.20

ODUSD(P) is in the process of development and presentation of an educational package on the new authority to withhold technical data and related evolving DoD policies to help assure effective implementation of this critical new program.

The OSD Steering Committee on National Security and Technology Transfer composed of representatives of many of the DoD components has been most instrumental in the development of these and other policies intended to address the technology transfer issues confronting the department today.

Our Foreign Disclosure and Technical Information System (FORDTIS) is playing an increas-

ing role in the technology transfer area. It is designed as a secure, automated information system to help the decision-maker and case-worker in processing strategic trade, munitions, and foreign disclosure cases by recording pertinent information.

Recent FORDTIS improvements are:

- The number of operational remote sites has increased from 12 (32 terminals) to 19 (60 terminals) in the past year.
- In 1983 FORDTIS became available for processing CCL and COCOM cases (FORDTIS had become available for commercial munitions license processing in 1982).
- Automated FORDTIS interfaces with State Department's COCOM Delegation in Paris became operational in December 1983.
- Progress toward identifying and implementing reference data bases has been made—all control lists (CCL—COCOM—USML) and the MCTL are now accessible in FORDTIS with cross referencing capability.
- Foreign availability, end user, and other data bases are being programmed for entry into FORDTIS and projected to be fully operational within the next year.

Further FORDTIS developments include improving analyst access to various agencies' data bases. The assimilation of specialized information from multiple sources, putting more terminals on line, and encouraging use of the data bases and system capabilities:

- For statistical analyses of substantive policy issues.
- To put better and more timely data in the hands of case processors.
- To allow better management control of the case handling process.
- To allow rapid assessments of the nominal end user as specified in the case and also whether equivalent or superior equipment can be obtained from Warsaw Pact or third world sources. (Most significant in our efforts to identify technology needing protection).

DoD Directive 2040.2 on international transfers of technology, goods, services and munitions was

signed by the Secretary of Defense on 17 January 1984, and provides a focused and balanced approach to the technology transfer issues before us. It states the Department's belief:

- That technology transfer is a critical national security issue.
- That the Department should treat "defense-related technology" as a national resource to be conserved in pursuit of national security objectives.
- That, consistent with these policies, it will apply export controls in a way that minimally interferes with the conduct of legitimate trade and scientific endeavor.
- The new directive, in addition to assigning technology transfer responsibilities within the Office of the Secretary of Defense, establishes the DoD international technology transfer (IT²) panel and subpanels (A and B):
 - The DoD IT² panel will identify and resolve technology transfer policy issues. It is chaired by the ASD (ISP)—the Honorable Richard Perle
 - The DoD IT² subpanel A will resolve DoD differences on matters referred to it concerning the transfer of technology, goods, services, and munitions. It is chaired by the DASD (IETSP), Dr. Stephen Bryen.
 - The DoD IT² subpanel B will resolve DoD differences regarding technical standards and definitions and the dissemination and exchange of information, it is chaired by the DUSD (R&AT), Dr. Edith Martin.
- Our office (ODUSD(P)) is represented on each of these panels and in the days ahead we look forward to the opportunity to make further contributions to the effort to diminish the threat to national security that is posed by unwanted and unintended technology transfer.

The Militarily Critical Technology List (MCTL) is still a classified document but efforts are continuing to bring about its sanitization and declassification.

- On 4 January of this year the Under Secretary of Defense (Research and Engineering) made another attempt to obtain the concurrence of the major DoD compo-

nents in the proposed declassification of the MCTL. In the form proposed, all the "rationale" statements for placement of a technology on the MCTL are deleted, as they constitute the identifiable items of classified information.

- Opposition to this approach remains; however, its essence is that the remainder of the MCTL would, in the aggregate, be a classified compilation of data.
- The current proposal to declassify the MCTL would go a step further. In addition to deletion of the "rationale" statements, the 17th and 18th chapters regarding nuclear technology and cryptologic technology would be deleted in their entirety. This proposal could go to the Secretary of Defense at any time now.
- An unclassified MCTL, of course, will facilitate informing people of those technologies the Department of Defense is concerned about. This is critical as we do not expect industry to control all technologies and not even all data about a given technology.
- Beyond an unclassified MCTL lies my hope that one day the department may even be able to reduce the size of the MCTL to something more manageable. A MCTL made up of the *most vital* technologies. A super MCTL perhaps.

Q. What can the Government do to me if I violate a certification made in order to get export-controlled data under your new regulations?

A. The answer depends upon the circumstances, of course. If you are not a DoD or USG contractor, there ordinarily would be little penalty other than cutting off your access to DoD-provided export-controlled technical data, i.e., you would no longer be a "qualified U.S. contractor." However, in such a case, if the violation of your certification involved a massive disclosure of militarily critical technology, the government might elect to prosecute under 18 U.S.C. 1001. If you were a DoD or USG contractor, a serious violation of your certification would be sufficient grounds for debarment action. You could also lose your status as a "qualified U.S. contractor", and there is still 18 U.S.C. 1001. Beyond those remedies there are the export control laws which, if violated, carry their own penalties upon conviction.

Q. Presuming that I am a "qualified U.S. contractor", do I have to have the financial capability to use your controlled technical data before you release it to me?

A. No. As the draft stands now, you would not have to make a separate certification about financial or technical capability to use the data. However, if you do not have such capabilities, and have no prospect of getting them, I would have to question why you need the data. What is your legitimate business purpose?

Q. Does this mean that I, as a "qualified U.S. contractor," have to have full technical capability to make use of the data in some legitimate business purpose?

A. No. You might very well depend on subcontractors who are also "qualified U.S. contractors."

Q. The proposed rules rely on DoD use of the Militarily Critical Technologies List (MCTL). How can I know what will be controlled when I cannot have access to the MCTL?

A. The MCTL is, of course, a classified document at present. Thus, it is not available to many people. Further, it is about 700 pages long. Notwithstanding, the Department of Defense must tell you what we expect to be controlled under the new rules. We will do this by marking the documentation in which the controlled information is contained. As indicated earlier, DoD Directive 5200.20 is being revised. Likely, when this process is finished, we will have another new distribution limitation statement ("G") that will match the distribution patterns of our new regulations.

Q. Based on your description of the new statutory authority to withhold technical data, it seems that the Department can withhold virtually any of its technical data. Is this correct?

A. You are close to being right. The statute does use the word "any" technical data. If the Department of Defense has the data, in all likelihood they have military or space application. (If the data does not have such application, one might ask why Defense has data without military or space application in the first place.) And, after all,

virtually everything is export-controlled to countries such as Cuba. But, this is why we are making use of the MCTL. It will serve as a screening device to enable our control of the most critical unclassified data; data that do not meet the MCTL test will fall through the screen and not be controlled under these regulations.

Q. Do your proposed regulations put the Department of Defense in the export-control business?

A. No. Both the State and Commerce Departments, in response to our first proposal that appeared in the Federal Register, reminded us that we have no charter to do so. Accordingly, certain parts of our proposal have been redrafted with that in mind.

**FOREIGN OWNERSHIP CONTROL & INFLUENCE
PAST, PRESENT & FUTURE—OBSERVATIONS**

**James J. Bagley
R. B. Associates, Inc.
and
G. Christopher Griner
Gardner, Carton & Douglas**

Again, it is a pleasure to address this body on a subject of continuing interest and of great importance to the defense posture of the United States—FOCI—foreign ownership, control and influence. In the time available I will speak of the past defined as up to the issuance of the Industrial Security Regulation February 1984. The present is from then until now, with comments on the changes. The future is any time after today.

This is the first opportunity to detail what is new with the hope that both government and non-government attendees will have a better understanding of the new era. If you wonder why I have the temerity to speak on the subject—well, those of you who know me also know that I have a habit of speaking on subjects of interest and also subjects of controversy. I hope that this exposition will result in a better understanding of what the rules and regulations are and how you might better view the subject of foreign involvement in defense matters. You have the problem and you must cope with it.

At the outset, a brief overview is appropriate to set the stage. All foreign relations and the basis for all defense relations stem from the White House, specifically the National Security Council (NSC). This body was most recently established by the National Security Act of 1947. It is the NSC which issues NDP-1 which establishes the criteria and policies on foreign disclosure.

There are also the export control laws which were enacted in 1949/1954 with the most recent, the Acts of 1979 on export administration which are now being debated in the Congress. In addition, and of great importance is the Atomic Energy Act of 1954, as well as the International Traffic in Arms Regulation administered by the Department of State; the current issue of which was published in 1976.

It is from those laws that the various international agreements evolve which are in addition to the various defense treaties: North Atlantic Treaty of 1949; Anzus, 1951; Southeast Asia, 1960; Japanese, 1960; Republic of Korea, 1953; and the Rio Treaty of 1947.

Note that these treaties cover a fairly long period of time. From these stem those exchange agreements that you are most familiar with: memorandums of understanding, data exchange agreements, foreign military sales, co-production agreements, etc. There are general security of information agreements with some 30 countries and industrial security agreements with a half dozen. The Department of Defense (DOD) has issued directives, the Military Departments (MILDEPS) have issued their implementing regulations and local commanders have added their own versions. Unfortunately, at the bottom of the pyramid is the Industrial Security Regulation and Industrial Security Manual. Lest there be any misunderstanding, the MILDEPS, and the heads of user agencies do have specific authority to issue and grant access to information under their cognizance under their own rules.

The FOCI Mechanisms—Past

THE PAST

**Laws, Regulations, Rules
—National Security Act of 1947, as amended
: National Security Council—NDP-1**

- Export Control Laws/ITAR
- Atomic Energy Act of 1954, as amended
- Treaties
 - : MOUs, DEAs, FMS,
 - : Agreements
 - General Security of Information Agreements
 - Industrial Security Protocols
- MILDEP Regulations
- Localisms
- ISR/ISM

FIGURE 1

Under the old regulations the only FOCI mechanisms were voting trust, proxy agreements and the reciprocal clearance. Under the voting trust process, the foreign owner turns over to a group of trustees, the total responsibility for the control of the operation of a company. The trustees were U.S. citizens, cleared or clearable who had no prior association either with the foreign owner or the company. In the proxy process, all stock is retained by the foreign shareholder, but a proxy is given to a trustee to vote the stock. The process was like the voting trust.

FOCI MECHANISM

- (1) Voting Trust/Proxy Agreements
- (2) Reciprocal Clearance

FIGURE 2

Limitation

LIMITATIONS

- (1) Foreign Disclosure
 - Is the information releasable?
 - Can/should the information be denied?
 - If so, how long?
 - Appeal mechanisms?

FIGURE 3

As I said earlier, the problem/limitation starts with: Is the information involved releasable to the country of residence of the owner? Can/should the information be denied? If so, for how long? Is there a mechanism by which a decision can be appealed?

Involved in this limitation was a diverse group of players—contracts, program, planners and security.

From a practical point of view each operated under a particular set of rules which ranged from: they knew what was releasable; they didn't know and didn't care because it was important to get a procurement package out. They cared, but did not know how to get the answer or from whom. They did not care what was disclosable. If it was to a foreigner—the answer is no, and don't confuse me with facts. So much for the limitation.

The Various Problems

Voting trusts/proxy agreements. The foreign owners had very few rights and no control over the actions or the destiny of a company they owned. Control had been vested in a group of U.S. citizens whom the foreign owner did not know. The owner had few of the prerogatives of ownership. From the U.S. point of view it was a good situation—control of the information was under U.S. control.

However, the trustees had problems which surfaced after it was discovered that they weren't paying much attention to the agreements of responsibility they had signed. The Defense Investigative Service (DIS) tightened the regulations to more closely reflect the existing Department of Defense Policy, and made the trustees responsible for their actions. Not all welcomed the changes. There have been no formal protests as far as I know, but it would not surprise me if some of the foreign owners with voting trust/proxy agreements would not apply for a change in status.

PROBLEMS

Problems—Voting Trusts/Proxy Agreements

- (1) The owners have few rights
 - (2) The owners have little control over the actions of trustees
 - (3) The Trustees were not happy
 - Too much personal responsibility
 - Difficult divisions of responsibility
- Government—owner

Problems—Reciprocal Clearances

- (1) Too little knowledge of the concept
- (2) Lack of consistency—application (even within commands)

- (3) Lack of disclosure decisions by SYSCOMS
- (4) Proliferation of NOFORN caveats
- (5) Difficult (impossible) visit procedure
- (6) If nothing is done—will go away.

FIGURE 4

The Reciprocal Clearance Process

The program has the best of intentions. It is a process by which access to classified information can be granted to individuals/facilities of governments which have entered into Industrial Security Agreements with the DOD. Originally, it was the UK and Canada. The Federal Republic of Germany was added later and there are others, principally NATO countries. There was high level interest in cooperation with our allies—rationalization, standardization and interoperability (RSI) became a "buzz word"; access would become easier. It didn't, in fact, it became more difficult. At the Orlando meeting (NCMS Vol XVIII-1982) there was a detailed exposition of the problems of trying to operate under the reciprocal clearance. In spite of the fact that cooperation was defined as being in the national interest and some reasonable rules were spelled out in the ISR/ISM, it is fair to say that the user agencies did not agree with the policy, disliked the concept and were not about to allow it to work. A voting trust or proxy agreement was OK. There was no foreign influence or control. Reciprocal clearance—No—we won't let it happen and, hopefully, the idea will go away.

I would like to reemphasize that through all of these problems DIS has been uniformly helpful, competent, and ever ready to solve problems.

Even when the companies concerned were representatives of our closest allies, were hi-tech companies, had provided goods and services to the DOD for years; in some cases were the sole supplier and were wanted by the program managers, it didn't make any difference. They were denied access to meetings, the information for industry briefings, to DTIC, to the information analysis centers and bid and proposal information. In addition, the current emphasis on technology transfer has compounded the problem.

There was a lack of consistency even within the same military department and even within the

same systems command. DD254s included language such as—holders of reciprocal clearances are not eligible for access to this procurement without the prior approval of _____. At times when an urgent appeal was made it was granted long after the closing date of the procurement action and could not be used as a precedent on future procurements in the same program. It is also pointed out that to make a formal protest under the DAR (or FAR) is not a viable solution for several reasons. Also, an appellant was not anxious to become known as a "whistle-blower."

In spite of the fact that regulations have limited the use of the term "NOFORN" (DODD 5200.15) there has been a substantial increase in the use of this caveat particularly when foreign-owned firms were involved. Even the Buy America Act was invoked.

Visits have been another nightmare. Regulations were issued by the MILDEPS requiring that a visit request of a U.S. citizen cleared by DISCO be processed through and approved by the embassy of the country concerned. The embassy of course did not have clearance information on U.S. citizens and were obliged to go back to DISCO for the clearance information in order to certify the visit. Fortunately, DISCO was cooperative. It is ironic that the ISM stated that the holder of a reciprocal clearance would be processed as a Category I visitor and the limitation on access noted on the request.

With all of this, there appeared to be an attitude in the user agencies of "the whole thing will go away." It didn't. People in high places rose up in righteous wrath and protested at the highest governmental levels—there was considerable press coverage—valid and invalid—on the problems on both sides of the Atlantic.

The Transition

As a result of the pressure for change, there was, at all levels a recognition that something had to be done. The political levels were concerned about the relations with our allies. Our allies were concerned about the sanctity of American commitments on mutual defense. American business was concerned about reciprocity—whether their firms operating in foreign countries would be given the same treatment as foreign

firms operating in the U.S. Unfortunately, in the words of the old mule skinner, to get the mule's attention a 2 x 4 is necessary. It is ironic that foreign owned firms of allies possessing technology needed by the U.S. military have difficulty getting authority for access.

Having given one side of the issue, there is another side that must be accepted and dealt with and that is whether the U.S. should be in a position of relying on a foreign owned firm for important defense equipment. Reliance for U.S. capability solely on a foreign owned source is an important national issue.

So it became obvious that there was a need for people to rethink the problem of FOCI to provide greater flexibility in the process, the need to recognize that inter-dependence was a fact of life and that even a foreign owner of a U.S. firm should and could have some rights. An important issue was whether it was possible to devise a system to operate within the framework of existing agreements, to protect sensitive information and to develop a system that could work. The result is the new FOCI policies published in the ISR of February 1984. These new policies are in Part-2—U.S. facilities that are foreign owned, controlled or influenced. The information is not in the ISM. Part 2 describes the acceptable methods of negotiating or eliminating risks associated with foreign ownership. I will briefly describe each and point out the change from the prior regulation.

Voting Trust. This arrangement provides for the exercise of the prerogatives of ownership by the trustees who will have complete freedom to act independently without consultation with, interference by, or influence from the foreign stockholders. The facility will be organized and structured and financed so as to be able to operate as a viable business independent from the foreign owners.

The trustees shall be U.S. citizens, residing in the U.S. capable of assuming full responsibility and exercising management responsibilities to ensure that the foreign owners are effectively insulated from the cleared facility. The trustees shall be completely disinterested individuals with no prior involvement in either the facility or the corporate body in which it is located, or the foreign interest, and must be eligible for and issued an appropriate level of clearance.

Proxy Agreement. The voting rights of stock owned by foreign interests are conveyed, in this option, to proxy holders by means of an irrevocable proxy agreement. Legal title of the stock remains with the foreign interest, all other provisions of the voting trust process apply.

You will note that the owner, for all practical purposes has relinquished virtually all rights to the facility he owns. The standard of responsibility for trustees and proxy holders under the Defense Voting Trust/Proxy Agreement is "gross negligence" not "ordinary negligence", as it is for a fiduciary or trustee in other trust situations. Thus, when there have been problems, and there have, the owner is left with considerable responsibility, but no rights. In one case, the trustees went to the owner for considerable financing for plant expansion and were not able to tell the owner why the financing was needed or what it was for.

Obviously, any owner would be reluctant to invest considerable amounts of money in an entity in which he has no authority to control. It is fair to say however, that in many cases the foreign owners are from countries with which the U.S. does not have a GSOIA and/or Industrial Security Agreement or, the owners have funds to invest and are not interested in controlling their investment.

Reciprocal Clearance. There is little change in the reciprocal clearance process in the new ISR. The DOD has entered into reciprocal agreements with several of its allies which establish arrangements whereby a contractor facility, which is under FOCI, located in either signatory country, may be eligible for access to classified information. A reciprocal clearance may be granted on satisfaction of the following criteria:

1. There is a reciprocal Industrial Security Agreement with the foreign government concerned;
2. A foreign business entity has a majority or controlling ownership of the U.S. firm, or a foreign interest effectively controls or has a dominant interest over the business management of the U.S. firm; and,
3. The facility does not require access to classified information which is not releasable to the foreign government from which the ownership stems.

THE PRESENT

- A. The Transition
 - The need for an alternative
 - Give the owner some control of his assets hire/fire/financial/policy
 - Protect U.S. interests
 - Limited option
 - National interest considerations
- B. Current Authorities
 - Voting Trust/proxy agreement
 - : No change
 - Reciprocal Clearance
 - : Limitations—no change
 - : Visit procedures—some improvement (visits to DTIC, Info Analysis Centers, Meetings not covered—still a problem)

FIGURE 5

You will find the specific access limitations in paragraph 31 of the ISM and you will note that there is no essential change in the criteria. There are, however, considerable changes in the visit procedures.

You might remember that the previous ISM designated holders of reciprocal clearances as Category 1. Visitors with the visit request indicating that the visitor's access was limited to the requirements of the ISM. That did not work. The MILDEPS issued their own regulations requiring, as said before, that the request for the visit be approved by the appropriate embassy concerned. Also, the holder of a reciprocal clearance was denied access to a broad range of information such as access to meetings, DTIC, bid, and bid proposal meetings, in fact, any meetings where classified information was involved.

Changes have been made in the visit procedures of the ISM which should improve the situation. No longer will the clearance be processed through the embassy. However I can see some pitfalls in critical areas of access which deserve attention.

Paragraph 41d(8) states in part: "Visit requests involving U.S. citizen employees of reciproally

cleared contractors (see paragraph 31) that required access to classified information or unclassified information related to a classified program or project and all visit requests involving foreign national employees of such firms, shall be processed to the UA Foreign Disclosure Office having jurisdiction over the information involved." Several questions and possible future problems come to mind:

- What about access to meetings such as those held under the auspices of such organizations as NSIA, AIA, ADPA?
- What about attendance at tri-service meetings such as the Tri-Service Laser Symposium, the Radar Symposium etc?
- How does this square with DoD policies on providing our allies with access to technical information (SECDEF Memorandum of 12 September 1983, "NATO/Allies Participation at DoD Related Conferences, Symposiums and Seminars?")
- Should this be considered in conflict with the policies outlined in SECDEF Memorandum of 18 October 1983, "Control of Unclassified Technology with Military Application?"

In all cases there are multiple sources of jurisdiction and multiple user agencies and programs involved.

There is another set of words which beg for clarification: "Classified or unclassified information related to a classified program." What is meant by unclassified? An announcement in the Commerce Business Daily? A DD254, which normally is unclassified? A classification guide? A request for a copy of an unclassified brief prepared for presentation to Congress?

What I am saying is that the problems of access for companies with reciprocal clearances have not gone away and have been exacerbated by the current verbage in the ISM when looked at in the light of the current problems on technology transfer. These are not frivolous questions particularly since there appears to be a high level desire to make international programs and processes work. And the reciprocal clearance process can work if the government players take the time and have the interest to make the process work. Again proper, complete and timely guidance is the single most important ingredient.

Special Security Agreement

This is a new option, one which may be used when a foreign interest owns a majority of the voting stock of a U.S. firm or if the holdings are sufficient to conclude that the foreign stockholders are in a position to control or have the dominant influence over the business management of the firm, and the foreign stockholders desire to retain some control over their assets.

Eligibility for this option requires that a user agency and OSD determination that approval will serve the national interest. The key issue is what is "national interest?" Industrial Security Bulletin 84B-1 of March 7, 1984 provided the following guidance to the cognizant security offices and is quoted in part:

"As a general rule, a favorable national interest determination includes an essential or impending prospective need to use, on a classified basis, the products, services, or technical expertise of a U.S. firm under FOCI when cleared or clearable firms are unavailable, or insufficient to satisfy industrial preparedness, mobilization, planning, research, production or production base requirement of a DOD component or a participating non-DOD user agency. The authority to make this determination is not permitted below the Assistant Secretary or comparable level of a DOD component or user agency concerned or his/her designee." The sole source situation speaks for itself. It is the other criteria that are difficult to define and determine.

SPECIAL SECURITY AGREEMENT (SSA)

- (1) Limits control by foreign parent
- (2) Parent, subsidiary and DOD execute the SSA:
 - SSA requires specific internal controls
 - : Classified information protected
 - : Performance on classified contracts assured
 - Failure to comply with SSA:
 - : Agreement cancelled
 - : Clearance of subsidiary revoked
- (3) OODEP Requirements:
 - Subsidiary established as a wholly-owned subsidiary of parent;

approximately 2 or more directors
(Proportions the key)

- : 3 outside directors—no prior relationship/employment with parent or subsidiary
 - Must be U.S. citizens—cleared or clearable
 - : 2 subsidiary representatives
 - Must be U.S. citizens—cleared or clearable
 - : 2 parent representatives. Excluded from access
- (4) Security Committee:
 - (The outside directors and subsidiary representatives will comprise the Defense Security Committee (DSC) to implement the SSA)
 - (5) Access by SSA holders:
 - Secret/confidential (see local DIS for details)
 - RD/FRD
(see also DOE FOCI of DOE Contractors, Federal Register Vol. 49, No. 41, February 29, 1984)
 - (6) Visits
 - Visitation Agreement:
 - Directed by DSC
 - : All representatives of parent must have prior approval of DSC for visits
 - Visits requests processed as Category I
 - ISM 41d. (8) does not apply

FIGURE 6

The SSA is a fully acceptable alternative to Voting Trust/Proxy Agreement arrangements, providing:

- The ownership stems from a country in which the U.S. has entered into a formal reciprocal clearance security agreement;
- All personnel required to be cleared in connection with the facility are U.S. citizens;
- The SSA may be considered for uses with companies from countries with a GSOIA or similar bilateral agreement provided:
 - All personnel required to be cleared are U.S. citizens; and
 - The facility clearance is limited to confidential.

Under an SSA:

- The foreign owners are authorized some control of the company.
- Specific OODEP requirements are established.
- In some cases the appointment of outside directors who must be U.S. citizens and cleared or clearable, similar to the voting trust option, are required.
- The outside directors and representatives of the cleared company subsidiary will comprise a Defense Security Committee (DSC) who will be responsible for implementing the requirements of the SSA.
- There may be representatives of the cleared subsidiary on the Board of Directors. They too must be U.S. citizens cleared or clearable.
- There are provisions which spell out in detail the authority of the foreign owners to control the affairs of the subsidiary.
- The parent may appoint representatives to sit on the board. They will be excluded from access to classified information in the possession of the subsidiary, except for that classified information which has been authorized for release to the government of the parent and further providing that the DOD has been provided security assurances for those individuals.
- Access by SSA holders (contact the local DIS for details).
- In general, the holder of an SSA will be authorized access to U.S. classified information in the same manner as the holder of a normal clearance:
 - Access to restricted data/formerly restricted data (see also DOE, FOCI of DOE Contractors, Federal Register, Vol. 49 No. 41, February 29, 1984) access would not be permitted to foreign nationals.
- Visits
 - The SSA will have a visitation agreement approved by the DOD which, in turn, will be directed by the DISC.
 - One of the elements of the agreement is that all representatives of the parent company must have their visit requests to the subsidiary approved in advance.
 - Visit requests processed as category I visitors.

- The requirements of paragraph 41d(8) of the ISM on the requirements for the holders of reciprocal clearances does not apply.
- DIS will annually review the SSA company for conformance with the requirements. The DSC will also complete annually a report to DIS on its actions in complying with the terms of the SSA.

Export Problems

- It is emphasized that the requirements of the export control laws and the ITAR will apply to any transfers of information between the subsidiary and the parent. The point is often overlooked: nothing you have heard negates the requirement for export control. Also, I would urge you to become familiar with the licensing requirements associated with visits, as well as the ISR requirements on international patent protocols.

It also should be noted that there are specific approvals required from the Department of State in licensing, patent and trade secret agreements involving the transmittal of U.S. classified information. There equally can be the same requirement for approval for the transfer of some unclassified technical data. (See also paragraph 21b of the ISM).

Summary

Having looked at the past and the present, it is obvious that there has been movement toward equity. But like any system that involves people and the problem of a rapidly changing world and, sadly, the resistance of people to movement and change, it is equally apparent that we must not and should not rest on our laurels and accomplishments, however great or small, but must be willing and ready to move ahead. So where are we?

The reciprocal clearance process is fundamentally sound. The process can work if you will let it. There has been movement and certainly a greater awareness of the problems. In the last few years there has been a substantial increase in the number of U.S. firms working around the work in defense matters and there has been a

substantial increase in the number of foreign companies doing business in the U.S.; the number of acquisitions of U.S. firms by foreign companies has grown markedly in the last two or three years, for example. The reasons are many and complex, but the bottom line is that there is an inter-independence in defense matters as well as purely commercial matters.

There is still a difference in the ways that we treat each other and it is fair to say that the treatment of U.S. firms in foreign countries is better than the treatment of foreign-owned firms in the U.S. and I assure you that it is not only that the foreign countries want U.S. technology; that is a simplistic view with diminishing credibility. If you will look at the number of military systems in our inventory from foreign sources you will see ample proof. So there is an inequity which can become serious unless continuing attention is given to it.

One of the underlying causes of the problem is in the foreign disclosure process. All programs and projects start at the applied research level. Basic research, which in the DoD must be militarily relevant, establishes the theoretical possibility that something can be done. In applied research, that possibility becomes a reality or is discarded. I could cite many examples of large current programs which started at levels of a few thousand and are now at the multimillion and higher. I submit that the key is a decision at the issuance of the first DD Form 254 for a small study contract whether there could be the possibility of foreign involvement in the program, if successful. And every reissue of that DD Form 254 should review that decision. When the program reaches the point that departmental or OSD approval is required, there will be a solid foundation for a decision to include or exclude foreign participation. I recommend to you the most recent report of Secretary Weinberger to the Congress on the "Standardization of Equipment Within NATO," January 1984. You will note also that the programs referenced to have been around for many years. The DoD has international cooperative programs with some 65 countries; the number of countries seems to be increasing.

Again, as you have been hearing for many years, correct and timely guidance is the key. It is distressing to see the number of security guides which have not been reviewed for several years

and the equally distressing conclusion that the attitude is to pass on some out-of-date and incomplete guidance to a contractor with the view: "Let him figure it out." And I am not overlooking the other side—when the contractor does take the initiative to submit his version—to ignore it or to take months for a decision.

Problems to be Addressed

FOCI will not go away. What is needed is a greater flexibility and a greater awareness that inter-dependence is a fact of life regardless of political persuasion or inclination.

THE FUTURE

A. Needs

- Foreign Disclosure Decisions at the R & D levels
DCP/POM Levels too late/decisions have been made
- Current/correct guidance
Frequent review of classification guidance
Specific guidance for subcontractor levels

B. Problems which should be addressed

- Whether international partners really are wanted?
- Will the number and scope of agreements be broadened as now apparent?
- If so, there is a need for greater flexibility at all levels.
- The need to import technology should be faced.
- NIH is still an important impediment.

FIGURE 7

Concluding Thoughts

Although there have been improvements in the FOCI process much more is needed:

- The reciprocal clearance does not work as well as intended. It can if you, the user agency, want it to work.
- The visit clearance problems have been addressed and improvements made, but it is still too cumbersome. The need is for greater decentralization of the decision-making process.

- With some exceptions the Voting Trust/Proxy Agreement process is not entirely satisfactory. I would predict that some of the owners who operate under such agreements will attempt movement toward a reciprocal clearance or special security agreement.
- The problems highlighted at every NCMS Seminar are still with us:
 - Better classification
 - More definitive/timely guidance
 - Consistency, consistency, consistency
- Some suggestions for consideration
 - (1) Review of existing directives for consistency, even the definitions are not consistent with each other
 - (2) Strategic trade. The recent introduction of the term "strategic trade cases" defined as "cases involving technology and goods that are dual-use in nature, that is, capable of being used either for legitimate civilian purposes or capable of being used or diverted to increase a nation's military potential."

CONCLUDING THOUGHTS.

- A. Although there have been improvements, much more is needed
 - Reciprocal clearances don't work as intended
 - Visit problems very cumbersome although some improvement
 - With some exceptions, Voting Trust/Proxy Agreements are not entirely satisfactory
- B. Problems highlighted at every NCMS Seminar—still with us.
 - Better classification
 - More definitive/timely guidance
 - Consistency within UAs

FIGURE 8

If you can think of any product which does not meet that definition, I would like to know. Just look at what you are wearing or carrying in your pockets, purses or briefcases and you probably will come up with a military use.

Representative of foreign interest. The definition should be reviewed as I believe it unrealistic.

For example, is an Officers, Owners, Directors and Executive Personnel (OODPEP) of a U.S. owned cleared company who is also an OODEP of a foreign company, not owned or controlled by a U.S. company, a foreign representative? Don't forget that the laws of some of our allies does not permit foreign ownership. This is a problem that should be addressed.

Finally, it is a fact that the U.S. is not necessarily the world leader in all areas of technology which have military uses. In his FY 1985 Annual Report to Congress, Under Secretary DeLauer cited the relative U.S./U.S.S.R. standing in the twenty most important basic technology areas, as has been done for the past few years. It is interesting reading. But the fact remains that international cooperation is a fact of life and will, in all probability, continue and increase annually.

SUGGESTIONS FOR IMPROVEMENT

- (1) Review of existing directives for consistency.
 - Even the definitions are not in agreement.
- (2) The current definition of "Representative of a Foreign Interest" should be reviewed. Does not recognize existing conditions.
- (3) There should be acceptance of the fact that international cooperation is a fact of life and will continue.
- (4) Although difficult, it should be recognized that the U.S. does not lead the world in new/advanced technology. NIH is not a useful virtue.

FIGURE 9

I hope that I have stirred up some controversy, as well as your thinking. As we have been saying for 20 seminars, the basic issue is classification—it is the key. I would urge that you obtain copies of all the back NCMS publications which are in DTIC. That is the only body of information available on this complicated, confusing, exasperating, exhilarating and fascinating subject—a subject which has been the source of much of the government controversy in the last 30 years. As a final word, the Freedom of Information Act will have its 18th birthday on July 4 this year.

TECHNOLOGY TRANSFER

James W. Dearlove
Defense Intelligence Agency
Washington, D.C.

I would like to talk to you for a few minutes on a topic that has been receiving a tremendous amount of publicity lately—one called technology transfer.

The technology transfer I am speaking of is the unwanted kind—that is technology transfer to our potential adversaries. There are many other kinds of technology transfer that are good. For example, from the industrialized countries to the lesser developed countries or from our space program to the field of medicine or aviation. However, I will not address these beneficial kinds—only the undesirable transfer—which can aid the military programs of our potential adversaries to the detriment of our national security.

There have been innumerable articles in the last year and especially in the last few months about past and present problems of technology transfer and what should be done about it.

Technology transfer is usually thought of as the sale or transfer of specific pieces of goods or equipment such as oil pipeline equipment, computers, equipment for the manufacture of trucks or aircraft, etc. I will talk about some of these but also other more subtle transfers, how they are accomplished and the end result of such transfer.

Technology transfer means different things to different groups. If you are a manufacturer or in the research and development world, it represents an item to be sold at a profit. If you represent the Department of Commerce, it could represent a method of establishing trade and equalizing your balance of payments. If you represent the State Department, it possibly represents a method of establishing diplomatic ties and linkage. If you represent the Department of Defense, technology most likely represents a national resource which should not be shared with potential adversaries for any reason. Perhaps there would not be so many different views of technology if we knew what technology and equipment was actually in the tunnel represented in the cartoon and if we knew precisely the use being made of whatever is in the tunnel.

The purpose of this talk is two-fold. First, to demonstrate that the Soviets and the east European countries have a concerted effort for the acquisition of Western technology and that this is a well-orchestrated, multi-faceted acquisition process beginning with open literature and continuing all the way through covert acquisition. Secondly, to outline for you how this system uses many mechanisms to achieve this goal. The Warsaw Pact acquisition process, we believe, is not only targeted against the U.S. but against all the industrialized nations of the world.

To highlight the Soviet view on this subject, I offer the following words from Leonid Brezhnev, "Science and technology have made it possible for us to create a powerful, qualitative new material and technical base. Our superiority in the latest types of military technology is a fact comrades, and one can't escape facts."

First, I would like to discuss the Soviet organization for technology transfer.

The directors of technology acquisition and its users are shown on Figure 1. The VPK, (the Military Industrial Commission) plays the major role in deciding what technologies are to have priority for acquisition. The users are the many defense industrial ministries and the other associated industrial ministries that also support the development and production of Soviet military equipment. (See Figure 1 at end of talk)

The GKNT (the State Committee for Science and Technology) with the assistance of several other countries is directly responsible for orchestrating the VPK priority requirements into the acquisition of scientific information, equipment, and instrumentation from foreign countries. The GKNT knows very well the deficiencies of the Soviet Union and, with the assistance of a number of organizations subordinate to it, knows precisely where to go to obtain the desired information, technology, and equipment—the country, the company, and if necessary, the individual. The GKNT negotiates scientific and technical contracts, bilateral exchanges and agreements with other countries as well as many individual companies. It also orchestrates the trade shows held in the Soviet Union and frequently extends invitations contingent upon the invited company's displaying specific pieces of equipment and

sometimes upon the condition that it be willing to sell the equipment from the floor. The GKNT determines the recipient facility in the Soviet Union and the price to be paid despite apparent evidence that various plants are bidding for the equipment. You will hear the name of the GKNT again throughout this presentation. It is not at all unusual for equipment being displayed to be taken apart and exploited or to be stolen from the display or to be stolen while in return shipment. There are many cases of outright theft of equipment and samples by the Warsaw Pact countries even from displays held in Western countries. (See Figure 2)

Several organizations supporting the GKNT and others enable them to perform their functions well. The most important of these institutions, the all-union Institute of Scientific and Technical Information (VINITI), has been described as the largest single producer of scientific and technical abstracts in the world. It selects information from a flood of domestic and foreign publications which it then analyzes and repackages for its users. VINITI reportedly controls about 10,000 scientific and technical libraries and receives annually 35,000 periodicals of various sorts, containing more than one and one-half million articles from about 125 countries in more than 65 languages and employs or has access to more than 150,000 persons. At the very minimum, this large effort is a great help in targeting emerging technology in the West. (See Figure 3)

Another Soviet organization involved in technical literature acquisition is the all-union Scientific and Technical Information Center (VNTIT). This information center is the equivalent of the U.S. Department of Commerce's National Technical Information Service (NTIS) and is principally responsible to the Soviet State Committee for Science and Technology (GKNT) and the Academy of Sciences. It is the ultimate recipient of all completed and in-progress Soviet technical project reports, conference and seminar proceedings, computer programs, engineering design documents and similar materials. It is also the registry for all Soviet research and development projects. Distribution of its holdings is restricted by a "need-to-know" basis in the Soviet Union. With this organization the Soviets are able to determine very precisely their strengths and their weaknesses. (See Figure 4)

The prestigious Academy of Science is responsible for conducting much of the basic research in the Soviet Union. However, it, too, is heavily involved in the effort to acquire western technology. Because it is labelled a scientific academy, it is able to open a great many doors throughout the world's academic communities, enabling it to serve as a very effective technology transfer mechanism. (See Figure 5)

Next, I would like to discuss some of the mechanisms of technology transfer. There are as many technology transfer mechanisms as there are ingenious minds. I have attempted to categorize some of the legal mechanisms on the figure below, beginning with various open literature publications and progressing through the various types of exchanges, business dealings, sales, exploitation of captured equipment and the use of Warsaw Pact nations as surrogates. There is the potential for any of these to be used illegally, as surely they are. There are numerous examples of technology transfer for all these mechanisms. My discussion will touch on only a few. (See Figure 6)

Turning now to illegal mechanisms, I have categorized below some of the more classic illegal transfer mechanisms including the usual spy cases, coopting of Western citizens and the use of communist controlled companies operating in the West. (See Figure 7)

There are many sources of information in the U.S. that feed the Soviet information gathering system. A select few are shown on this slide. NTIS, the National Technical Information Services, operated by the Department of Commerce, is the repository for most of the unclassified government R&D reports, these reports are available to the public without any dissemination restrictions. It has been, and still is, the recipient of documents that become unclassified through the general declassification schedule that we operated under prior to 1 August 1982. Until January of 1980, the Soviet Union had a standing order for one copy of every NTIS accession. That order was terminated as a sanction imposed because of the Soviet invasion of Afghanistan. However, the remaining Warsaw Pact countries can still receive these 80,000 documents per year and the Soviets can still order documents over the counter. (See Figure 8)

The Defense Technical Information Center is the repository for all DoD-generated reports and studies—classified and unclassified. The unclassified reports that have no further dissemination restrictions are automatically transferred to NTIS; so are reports that become declassified without further dissemination restriction.

Other publications, such as the Index of Security Classification Guides, which has been unclassified, enable potential adversaries to determine the title of practically classified weapons program of the DoD, thus providing an excellent spotting mechanism for further collection.

The Library of Congress, as the executive agent of a 19th century treaty, exchanges with more than 50 countries, including the Soviet Union, copies of all unclassified Government Printing Office publications, including Army, Navy, and Air Force field manuals.

In the area of national and international conferences, the Soviets are masters of the exploitation process. The Soviets sometimes spend as much as a year planning the exploitation of such conferences. Again, it is the State Committee for Science and Technology who orchestrates this exploitation. The U.S. Government has begun to look more closely at such conferences. In 1980, the Soviets and East European firms were denied access to a conference on lasers and a conference on magnetic bubble memory technology. From the concern over these two conferences, there evolved a government policy regarding open and closed conferences. If a conference meets the criteria for a closed conference, the sponsors of the conference must obtain a valid export license if delegates from proscribed countries are to attend. The most recent action to curb the flow of information through such conferences occurred in August of 1982. Approximately 700 papers had been prepared for presentation at two concurrent conferences on high speed photography and optics. At the insistence of the Department of Defense, approximately 120 papers were cancelled that were the result of research conducted by or for the DoD. Shown on Figure 9 are the titles of just a few of the papers that were cancelled. The U.K. also cancelled the papers of its representatives as well. This action averted what would have been a security disaster. It is safe to assume that this action and the attendant public-

ity attracted the attention of a very large number of persons and organizations and that future conferences of this type will also be reviewed for potential damage to security interests. A study of review and clearance procedures for government sponsored research has been conducted and regulations and directives are being implemented that will curtail the release of sensitive military-related information. (See Figure 9)

Soviet and East European firms known to be operating in the West provide an unparalleled opportunity for the acquisition of science and technology by legitimate means but also provide unlimited opportunities to illegally acquire all kinds of information and equipment, especially production-related equipment. Based on 1978 statistics obtained from a study conducted by Carleton University of Ottawa, Canada, there were more than 350 firms operating in the West that are co-owned or majority owned by the Soviets and East Europeans. Although the information on the slide indicates that 75 percent are engaged in export of raw materials, products, and technology, closer examination of their role reveals that many of them are also involved in, or are capable of, importing as well. Although the 396 million dollars invested in the 350 companies might appear significant, it is actually a rather insignificant amount for the tremendous returns these companies are able to provide in Western currency resulting from sales and the equipment and technology they are, in turn, able to buy with this currency. (See Figure 10)

Figure 11 shows the distribution of these Communist owned companies in the West. Omitted from the slide are any Western countries with less than 10 Communist controlled companies which accounts for the smaller total of 302 companies. (See Figure 11)

Since 1972, 10 government-to-government bilaterals have been negotiated between the U.S.S.R. and the U.S. At the U.S. president's direction, three were allowed to lapse in June and July 1982 as a sanction resulting from the Polish situation. These three were of greatest concern to the U.S., although all 10 have the potential for allowing the unwanted transfer of technology. Others may be allowed to lapse in the future. Activity under the auspices of the remaining bilateral agreements is now minimal. (See Figure 12)

There are numerous scholarly and academic exchanges and I will touch very briefly on these. The number of scientists involved in the inter-academy exchange is relatively small; however, very capable scientists from both sides are involved. There is ample evidence that all these exchanges are used to help fulfill Soviet deficiencies.

One of the provisions common to many of these government-to-government bilateral agreements encourages the establishment of separate agreements between individual companies in the West and entities of the Soviet government, principally, again, the State Committee for Science and Technology. These are sometimes referred to as the "Article IV" agreements because it is usually the fourth article in the agreement, and in the case of the U.S. these agreements have involved a large number of companies. These companies are among the world's leaders in areas in which the Soviets are deficient. The U.S. Export Administration Act of 1979 now requires that companies file notice with the U.S. Department of Commerce when such agreements are signed. We view these agreements as an excellent mechanism for the potential transfer of advanced technology. The meager information we have about "S&T Bilateral" agreements between our allies and the Soviets indicates that the same type of "Article IV's" are incorporated into those agreements as well. Indeed, the almost identical words shown on figure 13 were found in a 1969 bilateral agreement between the U.K. and the U.S.S.R. In December of 1981 and January of 1982, the Soviet newspapers, Pravda and Tass, both printed articles proclaiming that more than 30 such agreements existed with companies in the FRG. A cursory review of Soviet newspapers reveals that such "Article IV" agreements are signed with all industrialized countries with great regularity. (See Figure 13)

The graduate student/young faculty exchange is also used as a transfer mechanism—to the point that the U.S. now reviews many proposed programs, some of which are involved with critical military technology causing denial of the program which denies the student entry into the U.S. Restrictions are imposed on many more. Since 1978, the Senior Scholar Program has been used almost exclusively to attempt to send scientists and engineers to study in technical areas where the knowledge gained could have direct and

immediate military applications. Many of these applicants have been rejected, as well. East European students also attempt to study and conduct research in sensitive areas, but their applications, too, are closely scrutinized and rejected if necessary, with no distinction being made between Soviets and other East Europeans. (See Figure 14)

The Soviet students that come to the U.S. under the graduate student/young faculty program for a full academic year usually already possess the equivalent of a U.S. Ph.D. degree, average 34–35 years of age, and probably have about eight years of practical experience. The East European students follow a pattern very similar to that of the Soviets. The Soviet senior scholars originally came and conducted very basic research that was of little concern. Since about 1978, they have applied to conduct research in areas that also could be of immediate military benefit. (See Figure 15)

Examples of topics the Soviet students study are shown in Figure 15. I will discuss only one of these. In 1976–77, S.A. Gubin's course of study involved the technology of fuel-air explosives. Mr. Gubin studied this topic at one of our leading universities under a professor who was a consultant to the U.S. Navy for fuel-air explosives. Incidentally, during his stay Gubin ordered numerous unclassified government documents pertaining to fuel-air explosives. He undoubtedly returned to his fuel-air explosives work in the U.S.S.R. Gubin's true interests were not learned until several years after he had returned to the U.S.S.R.

Figure 16 is a photo of a port and the hundreds of items of containerized cargo which is illustrative of the problem of detecting and preventing the unwanted shipping of high technology. To combat this difficult problem the U.S. Customs Service is conducting operation "Project Exodus" which has been highly successful in focusing enforcement efforts. (See Figure 16)

Figure 17 is a picture taken from National Geographic Magazine, is a piece of equipment involved in a more recent attempt to evade the U.S. embargo. This is a piece of equipment used for high-pressure, low temperature oxidation process of manufacturing integrated circuits. It represents the very latest state-of-the-art used in chip

manufacture. Two such pieces of equipment were seized when a Communist-controlled company attempted to smuggle them out of the U.S. The value of the equipment was approximately \$500,000. The Soviets had authorized payment in excess, I repeat, *in excess*, of \$700,000 plus all expenses. (See Figure 17)

Along with the evasions, there are numerous actual and attempted diversions of equipment and technology. (A diversion being defined as an illegal use that occurs after the sale is consummated, without the foreknowledge of the seller.)

A case reported in the newspapers in 1981 involved one Peter Hermes of Hamburg who was apprehended while attempting to leave New York with an embargoed microwave receiver manufactured by the Micro-Tel Corporation of Baltimore, valued at \$49,000. The receiver was purchased by a naturalized American citizen of Soviet extraction, who provided it to Hermes. Hermes testified that he was paid \$10,000 to go to the U.S. and bring the receiver back to an individual by the name of Volker Nast of Hamburg, West Germany. Nast could not go to the U.S. in person to obtain the receiver because he has been charged in 1975 for conspiring to export several tons of embargoed electronic equipment used to manufacture integrated circuits. Both Nast and Werner Bruchhausen (famous in Silicon Valley diversion) have been tied to Richard Mueller who is involved in the recent computer diversion detected in Germany and Sweden.

William Bell, a former Hughes Aircraft engineer was arrested in June 1981 along with the president of a Polish-owned-U.S. chartered company for complicity in stealing classified U.S. Government documents about developmental radar systems. Bell's motive allegedly was financial difficulties. Figure 18 depicts some of the items that Bell provided information on. (See Figure 18)

Let us look now at the military consequences of some of these technology transfers. Unfortunately, the audit trail for much of the information and technology the Communist countries acquire is very difficult to follow. From the time an idea or a bit of information is acquired, incorporated into the Soviet system, goes through the complete research, development, test, and evaluation cycle and rolls off the assembly line, 20 years can

elapse. Nevertheless, there are a number of eye-catching examples that vividly illustrate the use of Western technology.

Shown in Figure 19 are just a few examples of some quantum advances the Soviets have been able to make because of ideas and equipment acquired from the West. A damage assessment of the Soviet advance in magnetic bubble memories for computers is that they would be 10 years behind the West today rather than only one year behind, had they not acquired the information by sending a Hungarian physicist to the U.S. (See Figure 19)

The second example is somewhat dated, but nevertheless, significant. In the late 1950s the U.S. and a number of other European nations openly published much of the technology relating to the chemical separation of plutonium from irradiated fuel elements using the solvent extraction method. This method was clearly superior to that of co-precipitation—the method employed at that time by the Soviets. We know the Soviets changed to this process as quickly as they possibly could. They immediately built new plants and abandoned construction on plants that were being constructed to use the older co-precipitation method. This immediately enabled much more efficient production of plutonium.

Many Soviet computers and electronic components are direct copies of Western equipment. I will not dwell on this subject but would like to point out at least two series of computers that are based on U.S. design. The RYAD ES-1020 which is based on the IBM 360. The Soviet SM-3 which is based on a computer of the Digital Equipment Corporation, the PDP-11.

Figure 20 shows a Soviet copy of the INTEL 2107 4K Dynamic Ram which very graphically illustrates a Soviet capability that we find is getting increasingly better, that of copying our micro circuits. Use of advanced western integrated circuits provides significant advantages in less weight and size while being able to handle increasingly more complex problems. (See Figure 20)

Similarly, the highly sophisticated Roll-On/Roll-Off (RO-RO) cargo ramp technology developed by France, but obtained through the Navire Company in Finland as well, has been incorporated

into the growing number of Soviet Roll-On/Roll-Off cargo ships. This technology is significant because the combination of sensors, cables and tensioners allows a steady ramp to exist between ship and pier, or ship and beach, enabling rapid unloading of heavy cargo (e.g., tanks) from ships. One of the very first uses of Soviet RO-RO ships was to deliver military supplies to Syria. (See Figure 21)

The U.S. YC-14 will not become operational but the Soviets are producing the AN-72 aircraft. (See Figure 22)

The IL-76 was copied from the plans of the U.S. C-141 which they had acquired. The Soviets extensively exploited the C-141 during a trip to Moscow and at two Paris air shows by photographing it, measuring it and even taking metal samples. The performance characteristics of the IL-76 and the C-141 aircraft are almost identical. (See Figure 23)

Next, I would like to direct your attention to the problems this legal and illegal technology transfer is causing the West. In addressing the cost to the West, first of all, let me say that no one, thus far, has been able to determine the total cost to the West of the technology that has been transferred to the East. When one considers the cost to the West, we must ask ourselves such typical questions as:

- What is the cost to the West that the Soviets now have a look-down, shoot-down capability? What new weapon system must we build to overcome this advantage?
- If the Soviets have developed a projectile that will penetrate the best armor available in the West, as they have claimed, what will it cost and how many years will it take to develop and deploy a Leopard or an M-1 tank with an improved armor system?
- Likewise, if, as the Soviets claim, they have developed an armor that cannot be defeated by Western anti-armor munitions what will it cost to develop and deploy new anti-armor systems?
- An even more difficult question would be what is the cost to the West of the Soviet research and development assets that are set free to work on military programs because the transfer of Western produc-

tion know-how frees their resources to allow them to work on problems of systems integration rather than component development and production?

- It has been stated that the sale of ball bearing grinders by the West (not just the U.S.—other countries have also sold ball bearing grinding machines) enabled the Soviets to increase the accuracy of their missiles. The point is not lost, that a comparatively minor sale can sometimes have profound and extremely costly implications—thousands, millions or possible thousands of millions times more than the short term profit that accrued from the sale. (See Figure 24)

This list of questions could be made endless. I do not profess to have answers to the above questions but let us look at some of the direct and immediate Soviet savings from technology transfer. From the facts available, we know the monetary savings to the Soviets can only be calculated in billions of dollars per year, when all the costs are considered—research, development, reduced life cycle costs, and the savings from removing obsolescent, costly systems from the field. In fact, we believe the savings in research alone could amount to billions per year.

The time saved by the Soviets in being able to pursue proven paths of research is enormous. While not every paper or idea that is transferred results in measurable savings of time, there is sufficient information to know beyond any reasonable doubt that such savings in time do accrue to the Soviets in far too many instances. This, of course, is tied directly to reduction of risk that enables them to overcome very significant deficiencies in a very short period of time.

Another item that must be factored into this cost versus savings equation is the fact that modern manufacturing equipment and machine tools enable the Soviets to reduce their production costs—enabling increased production or a lower overall budget than would exist otherwise.

The performance aspect has already been addressed to some extent in the series of rhetorical questions I cited above. However, let me make one final point. That point is that technology transfer fits in very well with the Soviets evolu-

tionary method of developing weapon systems, enabling them to insert proven concepts at any point in the life cycle of their weapons.

Finally, if nothing else, the acquisition of emerging technologies enables the Soviets to at least consider possible countermeasure options before the West can develop and deploy a weapon system. Certainly the acquisition of weapon systems, critical information about their mode of operation, or the acquisition of various components enhances their development of countermeasures.

This quote from a Soviet Communist summarizes their feelings on the use of Western technology, "The acquisition of Western technology and finished products is a very calculated procedure done with a great deal of selectivity. Even so, Soviet economists are amazed that the West does not recognize this and continues to invest in the U.S.S.R. industries since the material and technical base of socialism is thereby increased. They consider this acquisition program one of the U.S.S.R.'s greatest achievements since it allows the solving of complicated problems with minimal costs." Former Soviet Economist, 1976

In conclusion, there are major problems in the technology transfer area some are shown on Figure 25. (See Figure 25)

The greatest problem appears to be a lack of awareness. First, there is a lack of awareness of how dependent the Soviets are on Western technology and equipment. I have tried to convey to you some idea of how pervasive and how persistent they are in their technology acquisition efforts and how they use the transfer mechanisms I have discussed. You will recall that I discussed a number of mechanisms which can be summarized as:

1. Open literature,
2. Scientific and technical exchanges,
3. Students,
4. Legal purchases,
5. Espionage,
6. Co-opting our citizens,
7. The use of the East Europeans as surrogates,
8. The use of Warsaw Pact companies chartered in the West,

9. The complex network of evasions and diversions,
10. The acquisition from non-COCOM industrialized nations, and
11. The use of reverse engineering or direct copying.

The second awareness problem involves a lack of understanding that all these technology transfer mechanisms are centrally orchestrated and orchestrated very well.

Yet another awareness problem is that the average citizen as well as many persons in government fail to recognize the seriousness of this pervasive all-encompassing threat to our technology, thereby contributing to a lack of corrective action. Most persons have no idea how many Warsaw Pact visitors enter this country each year or how many are actually assigned here and even if they knew how many there were, they would not want to believe that someone was not watching them all the time. The information that I have presented has been presented to hundreds of audiences in our government and similar information has appeared in newspapers and magazines, and on TV and radio. The response received is always "Why isn't someone doing something about this problem?" or "How did we ever permit this problem to develop?"

This lack of awareness has caused inconsistencies to develop. There is an export control system. However, if everyone does not understand the total threat posed to Western technology by the many acquisition methods, and the damage that can result, such export controls can not be applied consistently to all the technology transfer mechanisms, some of which I just enumerated.

There may never be adequate resources or sufficiently high priorities to completely stop the unwanted flow of technology. However, I believe the rate of technology transfer can be slowed much more than it is at present. One of the major ways we can do this is to slow down the gratuitous transfer of openly available information. Our R&D personnel must realize that if they are producing a report that has high potential military value, that the unrestricted dissemination of such information is tantamount to serving it to our potential adversaries on a silver platter. Also, many

people must come to the realization that all our critical technology is not classified. Most of it is unclassified.

Until such a realization settles in, we are facing an uphill struggle to maintain our scientific superiority.

THE R&D PERFORMERS AND THEIR RELATIONSHIP IN THE SOVIET R&D PROCESS

Hierarchical Levels

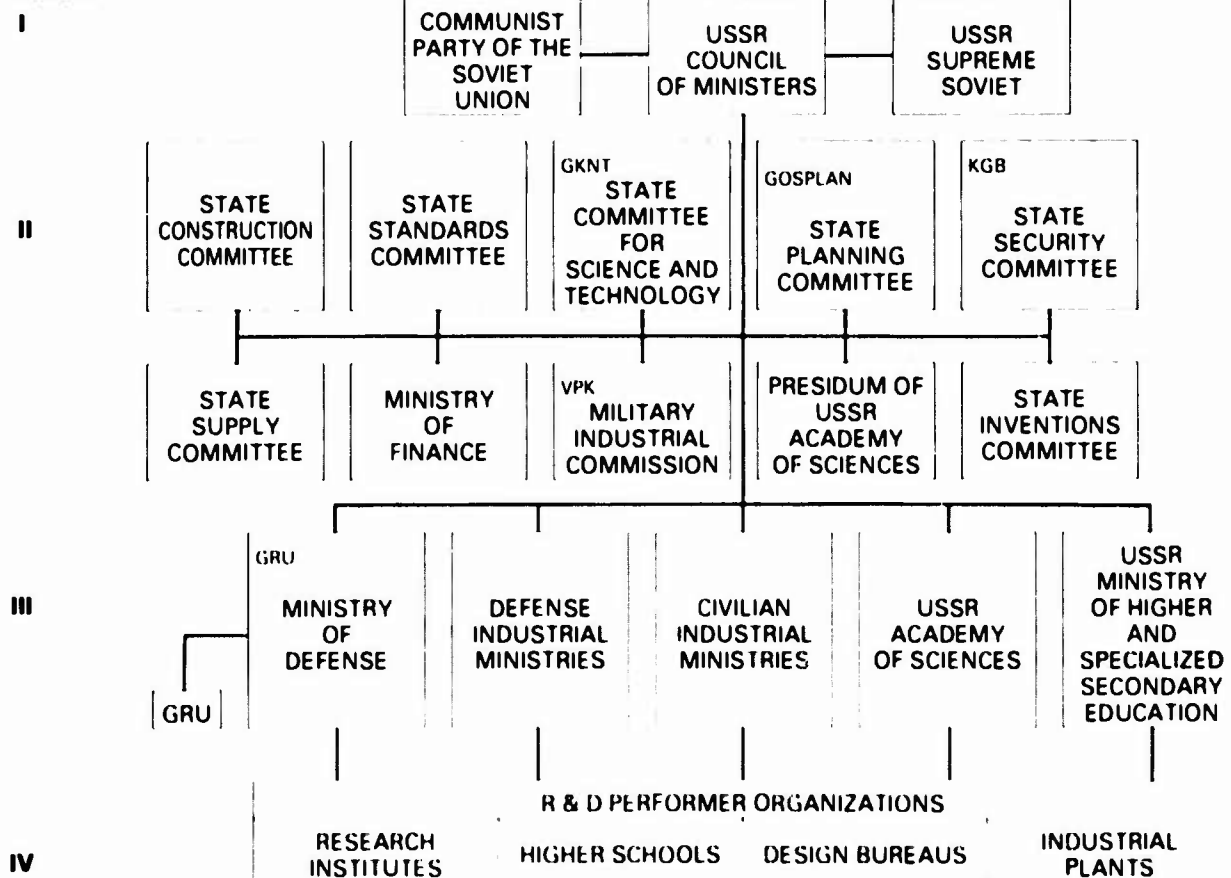


FIGURE 1

State Committee for Science and Technology (GKNT)

- **Maintains Priority Listing of Soviet Deficiencies**
- **Negotiates Scientific and Technical Contracts**
- **Negotiates Bilateral Agreements and Exchanges**
- **Works Closely with Academy of Science**
- **Orchestrates Trade Shows**

FIGURE 2

All-Union Institute of Scientific and Technical Information (VINITI)

- **Controls 10,000 Scientific and Technical Libraries**
- **Largest Single Producer of Scientific and Technical Abstracts in the World**
- **Receives 35,000 Periodicals**
 - **Containing 1,500,000 Articles**
 - **From 125 Countries**
 - **In 65 Languages**
- **Employs 100,000–150,000 Persons**

FIGURE 3

All-Union Scientific and Technical Information Center (VNTIT)

- **Receives:**
 - **All Completed and In-Progress Soviet Technical Project Reports**
 - **Conference and Seminar Proceedings**
 - **Computer Programs**
 - **Engineering Design Documents**
- **Registry for All Soviet R&D Projects**
- **Access Restricted to Soviet Government Projects Only**

FIGURE 4

The Academies of Science

- **Prestigious Organization for Scholarly Research**
- **Contains 450 Institutes, Scientific Councils, Committees, Laboratories and Commissions**
- **Maintains Numerous Exchange Agreements with Similar Academies or Agencies in Other Countries**
- **Works Closely with GKNT**
- **Collects Information In Fields of**
 - **Science**
 - **Social Science**
 - **Economics**
 - **Foreign Affairs**

FIGURE 5

Legal Technology Transfer Mechanisms

- | | |
|----------------------------------|--|
| • Scientific Publications | • Consultants |
| • Trade Publications | • Business Visitors |
| • Military Journals | • Salas Proposals |
| • Patents | • Legal Salas |
| • Data Bases | • Joint Ventures |
| • Conferences | • Third Country Salas |
| • Trade Shows | • Unembargoed Items |
| • Exchanges | • Equipment Exploitation |
| • Students | • Use of Warsaw Pact Surrogates |

FIGURE 6

Illegal Technology

Transfer Mechanisms

- **Evasions of U.S. Controls**
- **Diversions of Legal Sales**
- **Smuggling**
- **Illegal Purchases**
- **Clandestine Acquisitions**
- **Spying**
- **Ceopting Personnel**
- **Dummy Corporations**
- **Communist-Owned Firms in West**

FIGURE 7

Typical Sources of Information and Availability of U.S. Documents

- **National Technical Information Services (NTIS)**
 - **Unclassified and Declassified Government Documents**
 - **1,000-Plus Prepared Bibliographies**
 - **Computer Access**
- **Defense Technical Information Center (DTIC)**
 - **Unclassified Notices of Changes in Classification, Distribution and Availability**
- **Office of Secretary of Defense**
 - **Unclassified Index of Security Classification Guides**
- **Library of Congress**
 - **Exchanges All Unclassified Documents Printed by GPO**

FIGURE 8

Papers not Presented at Conferences on High Speed Photography and Optics

- Ship-to-Ship DF Laser Transmission
- Automatic Classification of Infrared Ship Imagery
- An Overview of Navy Robotics
- Advanced Automation for the Battlefield
- Compression of Forward Looking Infrared Imagery
- Reconnaissance in the F-18 Aircraft
- Infrared Digital Imagery System for Characterizing Battlefield Events
- Realtime Imaging Missile Tracker Simulation
- Integration of Aircraft and Satellite Imagery
- High-Speed Photography of Flaming Aluminum Particles Produced by a Rocket Propellant in an Acceleration Field

FIGURE 9

Soviet and East European Companies Operating in the West (1978)*

- 359 Soviet and East European Companies Operating in Western Countries**
 - 87 Percent Co-Owned or Majority Owned by Soviets and East Europeans
 - 75 Percent Engage Primarily in Promoting Exports of Raw Materials, Products and Technology
 - 50 Percent of Soviet Companies Located in Belgium, France, FRG and UK
 - 396 Million Dollars Invested in 359 Companies

*Source: East-West Project, Carleton University, Ottawa, 1979

**Does Not Include Offices of Intourist, Aeroflot or Chambers of Commerce

FIGURE 10

Number and Distribution of Soviet and East European Companies in the West (1978)

	AUSTRIA	BEL-LUX	CANADA	FRANCE	FRG	ITALY	NETHERLANDS	SWEDEN	UK	U.S.	TOTAL
BULGARIA	2	2	1	3	10	6	1	1	3	0	29
CSSR	1	2	4	5	2	2	1	3	10	0	30
GDR	3	2	0	3	1	1	2	2	6	0	20
HUNGARY	14	1	1	2	15	3	2	2	6	3	49
POLAND	7	6	2	7	15	2	3	5	12	15	74
ROMANIA	2	0	2	6	7	5	1	0	4	1	28
USSR	4	11	5	12	11	8	3	3	10	5	72
TOTAL	33	24	15	38	61	27	13	16	51	24	302

FIGURE 11

U.S./USSR Bilateral Agreements and Exchanges

Bilaterals

- S & T
- Space
- Energy
- Housing
- Agriculture
- Atomic Energy
- Environment
- Health, Heart & Med
- Transportation
- World Oceans

Exchanges

- National Academy of Science
- Graduate Students/Young Faculty
- Senior Scholars
- UN Fellows
- School-to-School
- American Council of Learned Societies
- Council for International Exchange of Scholars

FIGURE 12

Bilateral Agreements

Article IV

"Both parties will, as appropriate, encourage and facilitate the establishment and development of direct contacts and cooperation between agencies, organizations and firms of both countries and the conclusion, as appropriate, of implementing agreements for particular cooperative activities engaged in under this agreement."

FIGURE 13

U.S./USSR Student Exchange

- 40 Soviet Graduate Student/Young Faculty
 - 90% PhD Equivalents
 - 33-35 Years Old
 - 8 Years Experience
 - 90% Science or Engineering
- 15 Soviet Senior Scholars
 - Doctors of Science
 - Application Oriented
- Similar Programs with Eastern Europe

FIGURE 14

Soviets in U.S. Have Studied

- 76-77 S.A. Gubin
Passage of Shock Waves Through Inert and Combustible Heterogeneous Mixtures
- 79-80 K.V. Rozhdestvensky
Hydrodynamics of High-Speed Ships Using the Matched Expansions Method
- 79-80 V.V. Pilyugin
Computer Aided Design Systems-Computer Graphics
- 80-81 T.K. Bachmann
Selectivity of Visual Perception by Combined Psychophysical and Information Processing on the Basis of Automatized Systems

FIGURE 15

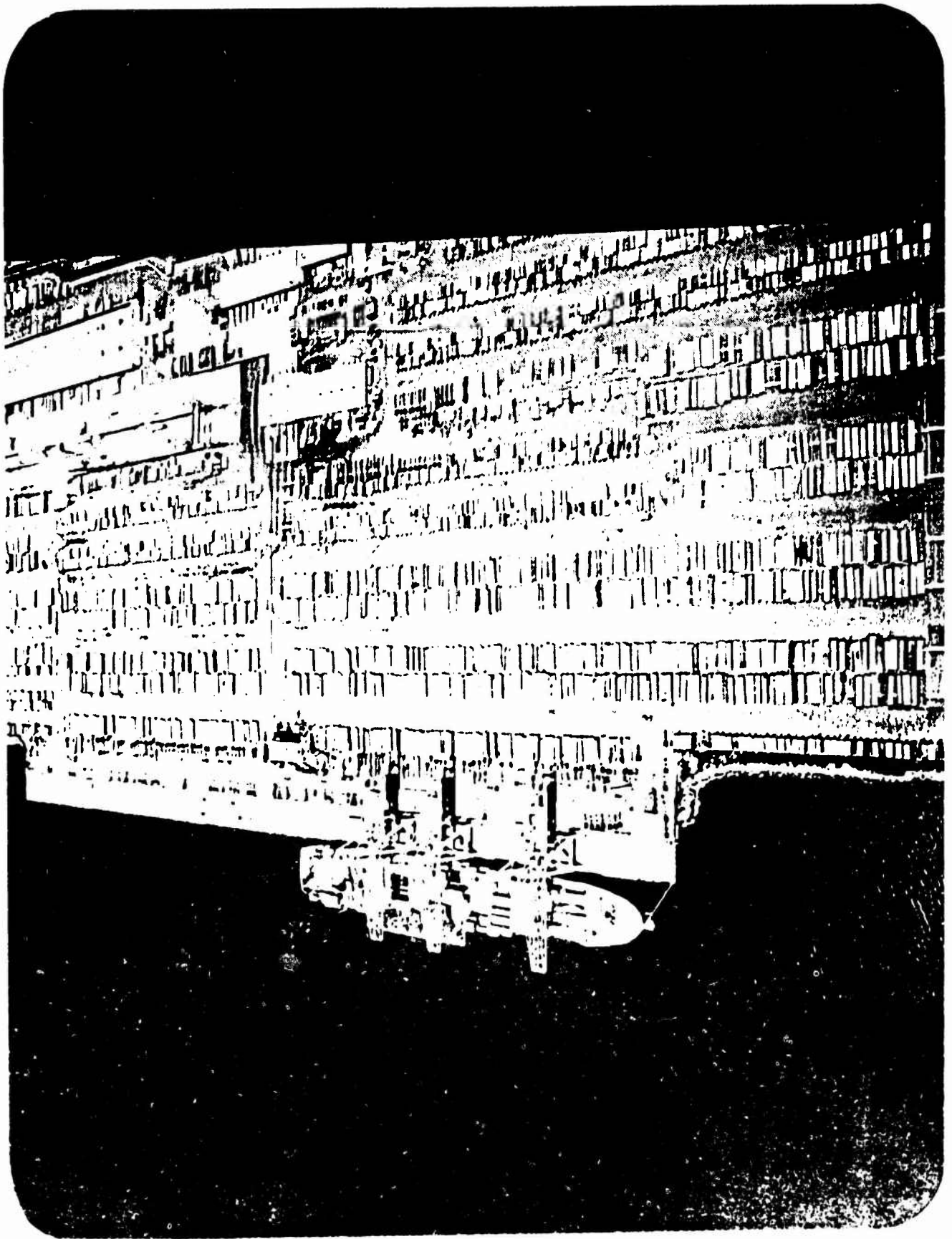


FIGURE 16

SEIZED MICROCIRCUIT MANUFACTURING EQUIPMENT



FIGURE 17

William H. Bell—Spy

- **Coopted by Polish Intelligence Officer Acting Under Cover as Vice President of Polamco**
- **Among Documents Compromised**
 - **F-15 Look-Down-Shoot-Down Radar**
 - **All-Weather Radar for Tanks**
 - **Information on Tow Anti-Tank Missile**
 - **Phoenix Air-to-Air Missile**
 - **Quiet Radar**
- **Bell received \$110,000**
- **Value of Information to Poles and Soviets—**
 - **Hundreds of Millions of Dollars in R&D Alone**

FIGURE 18

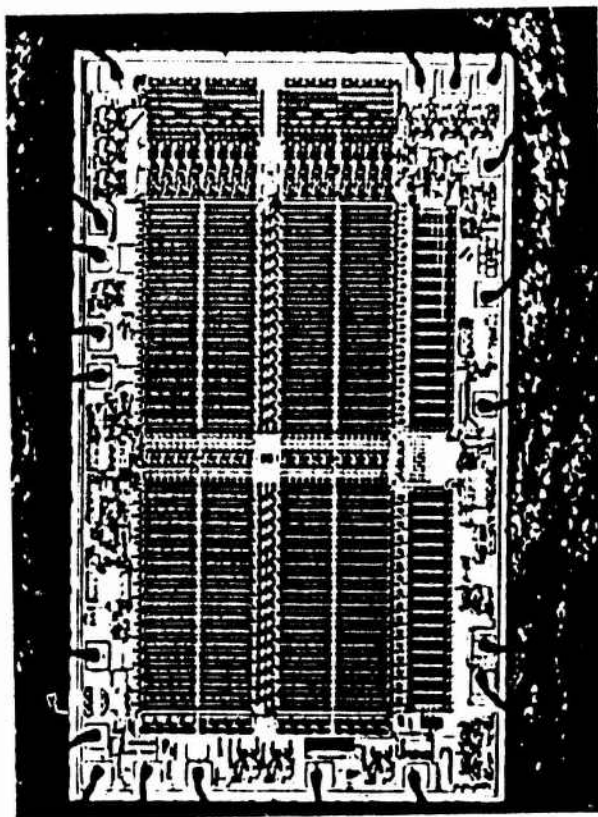
Quantum Advances from Technology Transfer

- **Magnetic Bubble Memory**
- **Chemical Separation of Nuclear Materials**
- **Chemical Warfare**
- **Microelectronics**
- **Computers**
- **Integrated Circuit Manufacturing**
- **Many Other Advances Derived from Computers and Microelectronics**

FIGURE 19

**Russian OK565PY1A
4K Dynamic Ram**

Length: .175" (4.45 mm)
Width: .109" (2.77 mm)



**INTEL 2107-B
4K Dynamic Ram**

Length: .174" (4.42 mm)
Width: .108" (2.74 mm)

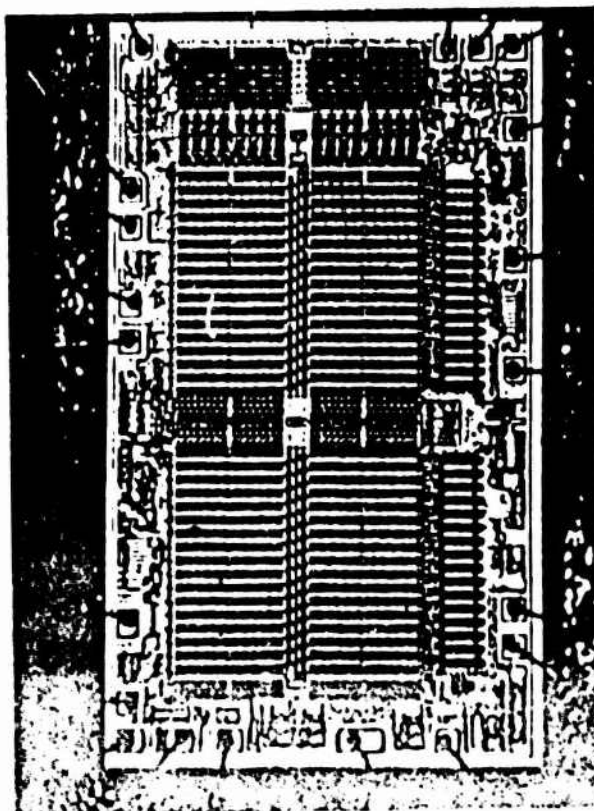


FIGURE 20

Soviet Roll-On/Roll-Off (RO/RO) Ship- French Built



Akademik Tupolev Class

FIGURE 21



YC-14



AN-72

FIGURE 22

C-141**IL-76****FIGURE 23**

Soviet Savings from Technology Transfer

- **Cost—Billions of Dollars**
- **Time—Up to 5 Years in R&D Cycle**
- **Risk—Tremendous Reduction—Reduces False Starts**
- **Plant Modernization—Reduces Production Costs**
- **Performance—Insertion of Proven Concepts in Evolutionary Development**
- **Countermeasures—Enables Faster Development**

FIGURE 24

TECHNOLOGY TRANSFER—A BRITISH PERSPECTIVE

John S. McMichael
Thorn EMI Electronics Ltd
England

Before starting my contribution on technology transfer I take this opportunity of bringing to NCMS members greetings from the Guild of Security Controllers. Last year at Fort Worth, I asked the Guild to explore the possibility of forming a closer association with NCMS. To this end, the idea was submitted to the Annual General Meeting (AGM) of the Guild held last October when the General Council was asked to investigate and put forward proposals to the membership at the next AGM. A committee of three was formed consisting of the three Guild international members of NCMS none other than Edward Atkinson of Ferranti Limited, who is here with us in Las Vegas, Bill Church of the Decca Company and myself. This committee has formulated proposals which will be referred to the membership and subsequently debated at the AGM next October. It is a longwinded process as we only meet once a year and I hope to be in a position thereafter to put proposals before your NCMS Board of Directors.

Now to the issue of a British perspective of technology transfer. I must first emphasize that I have no brief to represent either the U.K. Government or the U.K. Ministry of Defence. The contents of my presentation are my own views gleaned from many discussions held with business colleagues covering a wide spectrum of activities together with newspaper articles on the subject.

As you are well aware, security is essentially all about people and information, technology transfer concerning both aspects. My talk will deal with both these aspects and I hope it will show that we in the U.K. have been conscious of the sensitivity of and problems concerning technology transfer issues for many years. To go a long way back in history it appears that the Chinese were aware of this situation as far back as the time of Confucius as the following proverb attributed to him indicates: "A secret is your servant if you keep it, but your master if you lose it."

We in the U.K. share the U.S. concern about the illegal transfer of advanced militarily relevant

technology to the Eastern bloc, but where the scale of the U.S. home market can generally support an indigenous industry any individual European industry may be heavily dependent on an export market. Therefore, there is a more difficult balance to be struck in the case of U.K. industry between the need to control the export of high technology of strategic concern and the need to earn our living as a nation.

It would be hard to think of any area of advanced technology which does not have potential military applications. Our efforts must therefore be directed to controlling the flow of genuine military significant technology. Our ideas on this must be capable of revision on a regular basis to take account of rapid changes.

The U.S. and her allies have gone a long way in defining and refining the list of equipment requiring control, but this is the easier part of the exercise. Much the more difficult part of the task is defining the "know-how" which we are even more concerned to protect and once defined the means employed to protect it. It is one thing to devise a system of regulations and another matter entirely to enforce it as we know from your experiences during the "Prohibition Era."

The clandestine export of embargoed bulky equipment from the U.K. is probably rendered more difficult by virtue of the fact that we are an island but we would be deceiving ourselves if we believed that it is impossible. Most British firms are ready enough to accept the need to exercise control over what goes to the Soviet bloc and in general the U.K. government can count on their cooperation. However, British industry wants and needs freedom to trade with its allies and as much as possible with the rest of the free world with a degree of control which not only makes sense but is seen to be sensible.

The need as I and others perceive it is concentration on the areas of most concern as defined mutually between the U.K., the U.S. and their allies utilizing the machinery already established for this purpose.

In my role as a company security executive I am not privy to any covert operations which may be undertaken by government agencies to detect, deter and prevent the illegal transfer of technology

to the Sov-bloc countries. I am, however, well versed in the overt security measures taken to regularize the legal transfer of technology between our allies. Up to now, U.K. defence security measures, as they affect industry, are basically the same as those you take in the U.S. with the result that we maintain a common standard of approach to the problems. However, with the realization of the dangers arising from the illegal transfer of critical technology by devious means to our potential enemies, I feel that unnecessarily restrictive and impracticable protective measures may well be introduced which could result in damaging the cooperation and trust which exists between our respective countries.

I recall only too clearly during my first attendance at an NCMS seminar in Las Vegas in 1981, the worry expressed by many security veterans over the considerable losses of technology suffered by the U.S. due to the open publication of defence related technology. Considerable concern was voiced as to how these losses could be stemmed in the future. Three years later we are now experiencing measures which might enhance security but are having a profoundly adverse affect on business confidence in respect of the interchange of critical technology defence related or otherwise.

While it is likely that the Soviets may have acquired some useful technology from the U.K., some quite overtly, I do believe that specific security measures and procedures which U.K. industry has had to conform to over many years has limited the amount of technology which the Russians have acquired by legitimate means.

We erect security fences to minimum standards, install floodlighting, intruder detection systems, instigate control of entry procedures and enforce stringent methods of handling sensitive documents and hardware to name a few measures. These adequately deter the "honest" person but will not prevent the defences being breached by the determined intruder who will probably be firmly entrenched as an employee. Some businessmen have realized that there are many "fast bucks" to be made by the clandestine sale of hardware, technology and "know-how" cases which we have witnessed in recent years when a few of those indulging in this trade have been either brought to justice or exposed for the

villains they are. There were illegal shipments being apprehended almost at the border of the Soviet bloc. What we have seen to date may only be the tip of the iceberg.

As an illustration of awareness, I would like to recount an attempt to acquire information by fair and devious means. I recall an event back in 1971, when a Russian from the Soviet Trade Delegation in London, a Mr. Anatoly Makhov, appeared on my company's main site presenting himself to a receptionist. Because the receptionist was new to the firm she had good sense to refer him to the head office when he stated that the purpose of his visit was to acquire technical information or reports about magnetrons and valves which, he said, he had been able to obtain from his local public library.

On arrival in the head office he told the commissionaire what he wanted and was put in touch with the press relations officer. He was invited to take a seat in the foyer and given an in-house journal to read. The P.R. department provided some innocuous publicity material which would have been freely available had he written to or phoned the company.

When leaving the head office he asked the commissionaire, who was unaware of the nationality of the visitor, to direct him to the technical library which was situated nearby in a building where defence contracts were being undertaken. He was duly escorted to the building concerned and reported to the police post and was again asked to take a seat in the waiting room. A somewhat worried head librarian realized this visitor was a Russian and told him that the technical library was only accessible to company staff. However, if he cared to write to the company detailing the subjects in which he was interested, due consideration would be given to the request. Mr. Makhov then left.

A few weeks later one of those "further information" cards was received at the P.R. office seeking information on a number of topics about defence sensitive subjects. Again there was no joy forthcoming for Mr. Makhov and as you will see he made no bones about quoting his correct name and address on the card.

A few more weeks passed and then another "further information" card was received by the

company from a firm in the Royal County of Berkshire seeking information about a number of subjects, again defence related. The engineer who had dealt with the CCTV enquiry on the first "further information" card rang the managing director who had sent the second card to ask him to be more explicit as to his inquiry about CCTV. The managing director said he could not enlarge on the subject as he was applying on behalf of a Mr. Makhov of the Russian Trade Delegation! You ask what prompted Makhov to ask to be directed to the central library. On the in-house journal I referred to earlier, the words "supplied by the central library" were rubber stamped on the front cover—they are certainly opportunists when the situation arises. So much for Mr. Makhov's attempt to acquire defence technology. This incident does highlight the security awareness of all concerned.

To return to my earlier statement regarding the U.K.'s overt security measures, which go a long way towards protecting and controlling high technology, I will now enlarge on some of the measures involved so that you may have a better appreciation of the points I am making. First, I want to discuss a fundamental problem which no doubt causes you as much concern as it does the U.K. That is the vexed question of so called "academic freedom." There has always been and will continue to be a strong desire in the scientific world for the publication of thesis, research, project work and the like, any curtailment of which by planned safeguards will stifle it is claimed the creativity upon which our military and economic strengths rest. It is generally accepted in our defence security circles that within a defence oriented research organization it is desirable for there to be a degree of academic freedom based on a loose "need to know" principle in order to promote creativity and to cross fertilize ideas to obtain the best results—as the saying goes "Two heads are better than one."

For a number of years it has been my opinion that a company has more to lose financially by the loss of a commercial secret than it has by losing a military secret, no matter how damaging the latter event could be to the nation and no doubt the company concerned. I have found that company secrets are particularly closely guarded. Accordingly, it is my contention that for proprietary reasons, the disclosure of critical technol-

ogy to the Soviet Union is effectively blocked at the place of origin.

We have now come to the point where it is essential for there to be a sensible balance between openness and security which should be manageable through selectivity by pinpointing information where the perceived military needs of the Soviet Union are both real and confirmed by intelligence sources. In other words, we should be required to protect only that technology, know-how and/or hardware which is strictly defined as being of strategic use in the furtherance of the Soviets military capabilities.

In the U.K. defence industry many safeguards are inherent by virtue of government contractual obligations placed on companies whether or not classified matter is involved. Our much maligned Official Secrets Acts (OSA) 1911 to 1939 is applicable to all government contracts. A fact which is drawn to the attention of companies engaging in government work by reference to it in the contract schedule. Apart from drawing the contractor's attention to the OSA, it requires him to bring to the notice of all employees engaged on work connected with the contract the fact that provision of these statutes apply to them. For contracts involving information classified confidential or above, each and every employee employed on the contract is required to sign an undertaking confirming that his attention has been drawn to the provisions of the OSA. When leaving the company, he again signs a further undertaking reminding him of his original and continuing obligations under the act.

Another clause included in government contracts requires that a contractor may not disclose any information about any government contract other than to a person engaged in its performance even including information as to the existence of the contract. This clause also stipulates that except with consent in writing from the authority, the contractor shall not make use of the contract or any specification, plan, drawing etc., otherwise than for the purpose of manufacturing the articles. In other words, it is required that a company must obtain permission in writing to publically release any information, know-how and or technology about a contract.

Contracts involving the disclosure to a contractor of information classified confidential or above

are subject to a special security clause known as Standard Condition 59 which provides the legal and contractual backing for most of the defence security measures which a contractor is required to implement.

Apart from government defence contracts, firms sometimes engage in ventures which owe nothing to projects carried out under defence contracts or to any information which a firm has received from government sources. On the other hand such ventures do arise from defence contracts and/or information received from official sources. In either case the term used to describe these activities is "private venture." In the defence security sense it is used to describe project work or studies which appear to be of interest to a U.K. government department but which are not part of a government classified contract or sub-contract. Firms coming within the "private venture" field are usually already working in the defence field.

There is an obligation placed on defence contractors when they recognize a private venture project as having defence connotations to approach the Ministry of Defence (MOD) as early as possible to enable an assessment to be made of the potential market and to assure themselves that further development will not infringe their defence security obligations. In the event that a private venture project is deemed to require security protection the MOD will advise the firm of the classification to be applied.

On very rare occasions a private venture project with defence security connotations and undertaken outside the defence industry will arise and in this instance should come to the notice of MOD through patent action. As an example, this year such a situation arose when a U.K. computer company's device designed to prevent illegal copying of programs was judged to be sensitive by the government patent office who declared that the granting of the patent application in this instance would be "prejudicial to the defence of the realm." This brings me to the next subject concerning technology transfer—patents and designs.

The U.K. Patents Act of 1977 includes a provision that the publication of a patent application may be prohibited if publication is judged by the

competent authorities to be prejudicial to the safety of the realm or safety of the public. Publication is the very nature of patenting. This is similar to the Patent Secrecy clauses of your patent laws and is included in the U.K./U.S. Patent Exchange Agreement.

When a company submits a patent application which appears to the Comptroller of the Patent Office to be one of a class notified to him by the Secretary of State for Defence he may issue what is called a Prohibition Order which prohibits or restricts disclosure of information about the invention to which the application applies. While the prohibition is in force no patent is granted. Until the directions are withdrawn by the Comptroller of Patents the applicant is bound by the terms laid down—failure to comply with the terms constituting a criminal offense under the Patent Act. Similar provisions and penalties apply to the registration of designs under the Registered Designs Act of 1949. When a "prohibition order" is made the company's security executive concerned is notified by MOD Inventions Unit of the relative details. During the past twelve months I have had 28 prohibition orders referred to me. In prohibiting the granting of a patent application it is necessary for the authorities to strike a balance between possible damage to national security on the one hand and damage to trade on the other.

Under international agreements with many countries foreign patent applications can be filed in the U.K. in secrecy and vice versa.

I stressed earlier that the U.K. depends heavily on export markets not least in the defense field but before promoting the sale of a defence equipment to a foreign country authority to release the information involved to the government of the country concerned, classified or otherwise, must be sought through the Defence Sales Organization of the Procurement Executive MOD. The company's application must be detailed enough to enable the clearance authorities to process each case to the full. The reply to the application will specify the conditions and terms under which information may be released to the foreign government concerned. On the other hand, the reply may be a straight refusal to promote any equipment and there are many such decisions made. Any documents to be released as a result of an approved application are usually made subject to

and must clearly bear the MOD prescribed conditions of release.

I mentioned earlier that contractual requirements stipulate that defence contractors must apply to the contracting authority for approval before releasing any publicity material having direct or indirect bearing on any government contract or private venture project. Publicity material includes open publications, either in the press or at exhibitions, lectures, symposia or any other occasion where members of the general public have access to the information.

In addition to publicity matters there are, of course, comprehensive rules covering the display of defence equipment at trade fairs and exhibitions including events or open days at service or MOD establishments. Defence contractors must again obtain the written permission of the MOD to exhibit defence equipment and technology along with associated brochures, captions, press notices, films and other descriptive publicity literature. There are several other security requirements associated with the protection of the technology such as the safeguarding of classified features of the equipments. Provision must also be made to give security coverage while exhibits are in transit and during the open and closed hours of an exhibition. Staff manning a stand must be briefed as to their individual security responsibilities and so on.

I believe it is essential that you appreciate the point I made at the beginning of my discourse which is that the patriotic defence contractor will not knowingly permit the transfer of sensitive technology to the Soviets because quite apart from loyalty to his country and its allies the rules and regulations are such as to expose the wrong doer to breaking the law and face serious consequences.

I have not touched on the many other non-security controls that the defence contractor has to endure such as lists of embargoed equipment, import and export licenses, and user certificates to name but a few.

In conclusion, I submit that if our joint efforts to prevent genuine critical technology falling into the hands of the Soviets are going to succeed we will need to be absolutely clear as to what equip-

ment, know-how and technology we need to protect and by what means. In these times what is the latest technological development today could be old hat by tomorrow. The whole matter must be kept in perspective otherwise we will swamp ourselves with the sheer volume of uncontrolled effort to protect our technology. May I leave you with this thought which could also have been attributed to Confucius, "Information can be compared to perfume—once it escapes from the bottle it is lost forever."

TECHNOLOGY TRANSFER A CANADIAN PERSPECTIVE

Robert T. Grogan
Department of Supply and Service
Canada

Mr. Chairman, Ladies and Gentlemen, I wish to thank the Seminar Program Committee for inviting me to address you on the Canadian perspective regarding technology transfer. Having heard the previous speakers explain the United States and the United Kingdom perspectives, you will, no doubt, find my comments repetitive to some extent. I hope, however, that the distinctively Canadian aspect will prove informative, and will compensate, in that respect, for the lure of the pool and/or the casino at this late point in the afternoon.

Firstly, I would like to mention that Canada, as a trading nation, relies significantly on exports for its economic well-being. For example, two-way trade between Canada and the United States amounts to over \$100 billion per year. The importance of export sales by individual Canadian businesses, and to the economy as a whole, cannot be overstated. The Conference Board in Canada estimates that 20% of employment and 30% of the national production of goods and services are attributable to export sales. While Canada has usually been thought of as an exporter, in relation to agricultural and other natural resource products (largest portion of foreign sales), the export of manufactured products such as automobile and products with other high technological content are increasing. For instance, exports of aerospace technology (Canadarm, etc.) totalled an estimated \$1.7 billion last year. Exports of communications and related technology reached an estimated \$1.3 billion. Also proving to be highly

exportable is production technology in resources development.

I mentioned the foregoing, not to try to impress you with statistics, but to cast my future remarks in the context of the importance that technology (technical information and know-how in the production process, technical data and computer software) is playing and will continue to play in relation to Canada's economic and strategic health. Thus, we also must have mechanisms in place to ensure that our technology is only transferred offshore when it serves the national interest, and that technology belonging to allied countries that is transferred to the U.S. through international programs receives the level of protection (and security—if classified) prescribed by the country of origin. Our Department of National Defence (DND), for example, prescribes strict internal procedures for controlling access to DND technical information: received from allies; generated from in-house laboratory work; derived from work for DND by other government departments/agencies; developed from industrial contracts; and, developed from university research work.

Therefore, what classes or types of technological information do we Canadians see requiring protection or transfer controls? Currently our primary national legislation and guidelines are in relation to the control of technology transfer where the information is covered by the National Security Classification System, or the specific product is controlled by the Export and Import Permits Act (EIPA), or under our membership in the Coordinating Committee on Strategic Trade Controls (COCOM). Technological information may, in this regard, be conveniently divided into the following:

- *National Security.* This is information classified in the national security interest and protected by the security policies of the Federal Government and the Official Secrets Act.
- *Strategic Technology.* Technology which, although not always classified, might be considered strategic in nature and subject to the Export and Import Permits Act, or by reason of Canada's membership in COCOM.
- *National Interest Technology.* Technology uniquely of Canadian development at

Canadian expense that must be protected in the interests of employment and investment in this country.

- *Trade Secrets of Proprietary Information.* Information on technology provided by Canadian companies that they may wish to assign limited dissemination or, in some cases, none at all beyond government departments/agencies.
- *Open Technology.* Information on general technology that is in the interest of human progress to disseminate on as wide a basis as possible for the advancement of science.

We are of the opinion that technological information concerning national security, and strategic technology covered by COCOM, are adequately controlled by law and regulation. National interest technology and trade/proprietary information are not as specifically provided for (although considerable study of the problem is taking place) and realistic protection policies will undoubtedly follow. An across-the-board knowledge and understanding of the nature of the threats posed to high technology in Canada, and a broad awareness of the problems it poses for our national interests, presents difficulties. Our society, with very openly available scientific and technical information, is considered by certain nations (e.g., East bloc) as a mother lode of important information. For instance, it is generally recognized that, since the 1930's, the Soviet Union has devoted a major intelligence effort in this direction and, while it awards top priority to military and related technology, it is also interested in non-military industrial developments. In this regard, all expulsions of Soviet diplomats from Canada in the past two years have been for their activities in this area. In the area of national interest technology it should be remembered that Canada is actively competing with allied or friendly nations for the attainment of world markets for hi-tech products. Within Canada, as elsewhere, competing companies are naturally inquisitive about the developments of business rivals.

The threats to Canadian high technology can, therefore, be summarized:

- *Countries Whose Aims are Inimical to Canada.* That is, Warsaw Pact countries or states aligned with it or of similar persuasion.

Generally speaking, these are the so-called "scheduled countries." For these countries, Canada is a high target both for our own technologies and for those of our allies (e.g., United States and United Kingdom). In recent years, Canadian communications technology has been a recognized target.

- *Export Market Competitors.* The rivalry that exists in this area may be friendly, but we would be naive to believe that, when any country is striving to obtain exports to provide jobs for its workers, and returns on its R&D investment, it would not exploit advantages that arise. Such opportunities may well include international exchanges of technology. If Canada was to disseminate technology without reciprocity, or not show prudence in selecting or screening the technology we were prepared to disclose, we would do so at our peril. This threat could dull Canada's leading-edge in home-developed technology or, at worst, we could lose it completely.
- *Industrial Competition.* Individual companies spend considerable time and money on R&D and their owners or shareholders expect to see a return on that effort. Industrial security of proprietary information is understandably a major concern with Canadian industries in the hi-tech field. If Canadian government departments/agencies are to be a secure repository of company confidences, they must demonstrate the intent and the ability to safeguard company trade secrets (provided in confidence) against unauthorized disclosure. This is also provided for in law, whereby the head of a federal institution shall refuse to disclose the trade secrets of a third party (access to Information Act).
- *Personnel Security Threat.* This is a difficult threat to assess because it often lays with unintentional rather than malicious actions of individuals and impinges on the very real concern of the scientific and academic communities to publish the results of their research. Without adequate controls to protect Canadian interests, while ensuring maximum academic freedom, this could be the source of major problems in the protection of high technology.

Now, in relation to Canada's policy of controlling the export of military and strategic goods

(and, of course, the technology inherent in those products), I wish to describe the main legislation we have in place for that purpose, i.e., The Export and Import Permits Act (EIPA). It is the primary legislation controlling our exports, and the primary regulations made pursuant to the EIPA are: Export Control List; export permit regulations; trans-shipment regulations; and general export permit regulations.

The act provides for the establishment of an Export Control List (ECL) that includes any article the Governor-In-Council considers it necessary to control. The major reason for control relates to goods having a strategic nature or value which, if made available to certain destinations, their use might be detrimental to the security of Canada. For export control purposes, military and strategic goods have been broken into three categories:

- 1 Offensive military equipment;
- 2 Non-Offensive (defensive) military equipment; and
- 3 Other strategic equipment with possible military application.

Offensive and non-offensive military goods are systems or equipment specifically designed for military use and include any system or device capable of enabling an attack to be delivered (i.e., combat aircraft, armoured vehicles, arms and ammunition, as well as other equipment such as transport aircraft, communications systems, navigation devices, etc.) when built to military specifications. This also includes specially designed component parts for such equipment. Other strategic goods are equipment of a commercial civilian nature that could have military application (i.e., computers, telecommunication systems and most civilian aircraft and associated equipment).

Any goods that fall within the above categories, and are identified on the Export Control List, are subject to control and require an export permit prior to shipment from Canada to any destination (except, in most cases, the United States). Unlike many other provisions of the Act, the policy that forms the basis for the implementation of controls in this area is set out in a 1978 Canadian policy that essentially re-affirmed an approach developed in 1970. Provisions of the policy are based on the principles that military and strategic

equipment should generally not be supplied to: countries considered to represent a military threat to Canada and its allies; countries to which United Nations resolutions forbid the export of arms; countries involved in or under imminent threat of hostilities; and regimes considered to be wholly repugnant to Canadian values, especially where such equipment could be used against the civilian population.

The first of these provisions is based upon national security concerns. The remainder reflect foreign policy or political considerations. To implement the above objectives, interdepartmental procedures were also established under the policy and authorized by the Canadian government to provide for a case-by-case review of proposed exports where political or security concerns may arise.

Other reasons for control under the EIPA are as follows: to promote further processing in Canada of a natural resource; to limit the export of any raw or processed material; to implement an intergovernmental arrangement; and to ensure an adequate supply of articles in Canada for defence or other needs.

The Export Control List (ECL) is comprised of ten groups similar to the U.S. Commodity Control List and Munitions List. Several of these groups correspond to COCOM Lists. One group (Atomic Energy Materials and Equipment) has included both for security reasons and in fulfillment of Canada's obligations under the Nuclear Non-Proliferation Treaty.

Under the ECL, the Export of Technology, Item 10003 applies to technical data in material form (such as drawings, photographic negatives and prints, recordings, design data and manuals) that can be used in the design, production, operation or testing of equipment and materials described in certain groups of the ECL. If such technology is related to U.S. goods, Canada would normally seek U.S. concurrence before issuing an export permit, the control does not, however, apply to: technical data in immaterial form (such as the exchange of thought between experts); technical data in material form that can be used in the design, production, operation or testing of unlisted equipment or materials; or, data available to the public in published books and periodicals.

Under section 3 of the EIPA the Act specifies that the Governor-in-Council may establish a list of countries, to be called an Area Control List (ACL), to which the export of goods should be controlled. The power to create or to amend such a list is a very broad one and there are no legislative criteria restricting the use of this power. Permits must be obtained for the shipment of the majority of goods, whether appearing on the Export Control List or not, to countries designated on the Area Control List. Traditionally, countries have been named to this list on the basis of national security concerns. The list includes the Warsaw Pact countries, Albania, North Korea, Mongolia and Vietnam and, until recently, the People's Republic of China. The countries appearing on the Area Control List (plus the PRC) embraces those countries that Canada, as a member of COCOM, has agreed that a multilateral system of controls should apply to in order to limit or prevent the acquisition by these countries of advanced military and strategic goods and technology. In practice, export permits would not generally be issued for the sale to any Area Control List country of any goods that may have a military application.

Canadian policy categorizes countries based on their sensitivity:

- Group A—Least Restrictive
- Group B—Most Restrictive
- Group C—May range from least to most restrictive

Generally, offensive and non-offensive military equipment are not approved for export to Group B countries, but there are exceptions. Exceptions are considered on the basis of changing political and security considerations.

The ECL has an item dealing with goods of U.S. origin (9001) by a formal agreement between the Canadian and U.S. governments. Under the so-called Hyde Park Agreement of 1941, the application of strategic export controls between the two countries was suspended and was replaced by a separate system of controls on re-exports from each country of goods originating in the other country. It was to implement this alternative system of controls that a specific item of the ECL was created. U.S. origin goods, as defined in that item, may be re-exported from Canada if the

export would be approved under U.S. Law (i.e., no licence required or no objection). If Canada determines that U.S. regulations have restrictions for certain U.S. products to certain destinations, we seek the U.S. views, either formally via the Embassy or informally via direct contact with the Department of Commerce. We do, however, also refuse export permits outright.

In relation to control over previously exported Canadian products, Canadian legislation, per se, does not permit the direct control over a subsidiary or other firm based in a foreign country to abide by direct Canadian government control. However, in instances where there is transfer of technology, the Canadian government imposes restrictions on third party sales of the equipment and technology through contractual obligations between the Canadian exporter and the foreign importer/user of such technology. In other words, the contract entered into between the parties generally stipulates that, prior to the foreign manufacturer initiating third party sales of either the technology or the equipment produced from that technology, he must first seek the approval of the Canadian licensor who in turn will seek the approval of Canadian government authorities.

At the same time that our government categorized equipment for export under the ECL, it also identified countries into three groups based on their levels of sensitivity:

- (I) Category I, II, or III equipment when destined for Group A countries are rarely consulted on—in other words, approval is generally given at the divisional level.
- (II) Category I and II equipment, although normally not approved for export to Group B countries, is subject to an intensive inter/intradepartmental review process.
- (III) Category III equipment, on the other hand, to Group B countries are subject to the same intensive review process as that undertaken for Category I and II equipment if such equipment is or may be destined for military end use.
- (IV) Category I equipment to Group C countries is always subject to the same intensive review process.
- (V) Category II equipment is reviewed inter/intradepartmentally if the value exceeds \$100,000.

- (VI) Category III equipment, on the other hand, is generally approved for export at the divisional level although depending on the sensitivity of the country at any particular point in time, inter/intradepartmental review will be initiated.

Applications to export certain equipment and technology to certain countries are subject to an intensive inter/intradepartmental review. There are two departments primarily involved in this review process. They are the Department of National Defense and the Department of External Affairs.

National Defense is specifically concerned with the military security of Canada and its allies and will advise on any implications which could be detrimental to Canada's national security interests. It also conducts a thorough intelligence analysis of proposed exports and will advise if there appears to be discrepancies in information provided by the applicant for an export permit or if there is information that would contradict intended end-use.

The Department of External Affairs review process is an extensive one and somewhat analogous to that conducted by DND, although the concerns do vary. These address:

- Political Aspects—Generally this review is conducted in relation to Canadian foreign policy interests and provides input into the implications for Canada of any sales of military and military-related equipment.
- Defence Relations—Provides assessment of such sales to a specific country which may impact on our bilateral and multilateral relations and obligations in the defence area.
- Defence Programs—Advises as to the consequences for Canadian companies if certain exports of military and military-related equipment are refused to specific destinations.
- Intelligence—The External Affairs Intelligence Bureau reviews applications in light of their intelligence analysis from a Canadian foreign policy perspective.
- Trade Economic—The different bureaus we consult with will advise on the economic

and trade benefit which will accrue to Canada should approval be given.

- Human Rights—Will advise on whether certain exports would conflict with Canada's policy relating to respect for human rights and especially whether such equipment could be used against the civilian population.

When the review is completed, if there are no objections raised, the permit is issued subject to any import certificate or end-use certificate requirements. If objections are raised in the process, the Secretary of State for External Affairs (SSEA) is requested to decide on whether the permit should be issued. The SSEA is consulted and his decision is also sought in all very sensitive cases and when the economic value of the proposed export is especially significant.

In respect of export permit procedures for proscribed destinations, all general exception/administrative exception goods to proscribed destinations which may have security concerns are referred to DND for security/intelligence review. If the general exception is approved by DND, the case is forwarded to COCOM (on occasion DEA consult with other offices, as necessary).

If administrative exception is approved by DND, the general consultation procedures apply (i.e., DND, DEA—political, trade/economic, human rights, intelligence—defense relations).

The other legislative basis of our export control program is the Customs Act. The Customs Act authorizes customs officers to detain goods, the export and import of which is controlled under any act of Parliament. Customs assists the Department of External Affairs in the administration and the enforcement of the Export and Import Permits Act. From an administrative enforcement standpoint, customs assistance with respect to export controls includes the following:

- 1) Notifying customs ports of exit of pertinent legislative requirements (controlled status of export shipments and export permits) and any changes made to such requirements from time to time.
- 2) Verifying the export documentation (i.e., export permits and Canada customs export declarations) for compliance.

- 3) Detaining suspect shipments where practicable for determination of permit requirements by the Department of External Affairs.

In order to ensure that voluntary compliance is not abused, from time to time, customs conducts an in-depth examination/audit of export documentation. On occasion, however, physical examination of shipments for exports are carried out. This is done in special circumstances associated with, for example, required but missing export permits, incomplete permits, or if the goods to be exported are "on lookout." Customs administrative and enforcement activities are further enhanced by its investigative and intelligence services.

Investigative Services

Customs officers are responsible for the investigation of suspected violations and the enforcement of the Export and Import Permits Act. Customs officers include designated members of the Department of National Revenue, Customs and Excise, and the Royal Canadian Mounted Police (R.C.M.P.) Customs and Excise branch.

Generally, when information becomes available to either party that an export-related contravention of the Export and Import Permits Act has occurred, Customs, External Affairs and the RCMP will consult on the merits of carrying out an investigation and, where evidence supports investigative action, this is undertaken with cooperation between the parties. In order to maximize the level of cooperation and clarify "gray areas."

Regarding intelligence services and information exchange, the adoption by Canada of the recommendations of the Customs Cooperation Council (CCC) enables it to enter into the exchange of information with member countries. Revenue Canada, Customs and Excise, adheres to the principles of the CCC respecting information sharing. Customs exchanges information on a general basis and on specific matters as requested. As well, customs exchanges analytical reports with certain countries on topics such as:

- Potential or actual risk situations at the tactical and strategic level;
- The Modus Operandi; and,

- Evasionary methods and conveyance routes used or likely to be used by offenders.

One of the major means of collation of data for customs is a computerized system known as AICS (Automated Intelligence Customs Service) which is shared with the RCMP, Customs and Excise branch. While the system is currently not "on-line", in that terminals are not deployed in the field, AICS makes a valuable contribution in providing an excellent data base for monitoring and enforcement purposes.

Customs cooperates on an on-going basis with its U.S. counterpart. The extent of such cooperation is evidenced by information sharing on day-to-day operations, sharing of selected data in the AICS data bank, and providing informational support to U.S. customs on projects such as "Operation Exodus." Customs is continually looking for ways to enhance its data base and to share information gathered on a selective basis with member countries. As an example, customs is currently negotiating a new bilateral agreement with U.S. customs which, among other things, will in all likelihood, result in increased mutual assistance and sharing of certain information between the two organizations.

In March 1983, National Revenue, Customs, and Excise created the directorate of "Commercial Verification and Enforcement" to provide a focal point for Commercial Verification and Enforcement activities in the department. The directorate is responsible for designing, developing, testing and planning the implementation of policies and programs for the effective detection of illicit international movement of commercial goods and related enforcement policies. The program development for export controls falls within these responsibilities. Customs is reviewing their present export control program as part of a general review of commercial enforcement policies and programs. In this respect, they are examining investigative techniques from other enforcement programs, including the U.S. "Exodus" program, for their application to any increased export control program they may develop.

Ladies and gentlemen, I sincerely thank you for your attentiveness during this protracted presentation. In closing, let me leave you with the clear

understanding that the government of Canada is committed to maintaining the technological superiority of the West in military equipment and also the broader, more advanced underlying technology and industrial base.

We have legislative and other mechanisms in place to support that commitment and we are currently examining other ways and means by which the export of sensitive high-technology products can be better controlled to prevent that technology from reaching those who do not wish us well. Thank you.

COMPUTER ABUSE AND THE HACKER

David C. Brown
Federal Bureau of Investigation

Hacker's anthem

"Put another password in,
Bomb it out, then try again.
Try to get past logging in,
We're hacking, hacking, hacking.

"Try his first wife's maiden name,
This is more than just a game.
It's real fun, but just the same
It's hacking, hacking, hacking."

The month of August 1983, was a banner time for writers of editorial headlines:

"A secret battle: Security hackers vs. big computers"

"Computer whizzes dial up a secret U.S. code"

And, perhaps, the more rational,

"Teen Computer break-ins: High-Tech Rite of Passage."

What's the excitement? Computer hackers. Specifically, a group of youngsters in Milwaukee, Wisconsin, who used their home computers, modems and moderate knowledge to access computer data bases of a hospital, a bank, some private businesses and—as one newspaper described it—"... a computer at America's top-secret nuclear weapons research laboratory."

The FBI investigated the Milwaukee case, utilizing the federal laws that most closely applied to this act. From that investigation, interviews with a large number of hackers and involvement in other cases of computer abuse by hackers, a number of important issues have been raised. Certainly, we have found a greater number of questions than answers. But, our attention is more focused. The perspective of federal law enforcement toward the general problem of computer crime is becoming sharper, and the FBI's view of the hacker is a part of that trend. Interest and investigation, however, are two separate matters, and the lack of specific federal sanctions concerning the unauthorized entry into a computer data base greatly limits the FBI's investigative interest. For, without the allegation of a violation of federal law, no investigation can commence. Further, the criminal statutes rightly make no allowance for investigating U.S. citizens in the absence of a violation of law, even when the acts being committed represent an invasion of the privacy of others.

The difficulty of investigating and prosecuting computer abuse cases was pointed out by Mr. John C. Keeney, Deputy Assistant Attorney General, Criminal Division, in his testimony before a Senate subcommittee regarding computer fraud. Mr. Keeney observed that, "Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent and then the prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets. The crafting of such a theory can be awkward, and the results far from perfect."

There are a number of bills being considered on Capitol Hill to attempt to bring about federal legislation concerning computer abuse. The best known are probably Rep. Bill Nelson's HB 1092, the Federal Computer Systems Protection Act (sponsored in the Senate as SB 1733 by Sen. Paul Trible) and Rep. Ron Wyden's HB 3075, the Small Business Computer Crime Prevention Act. The thrust of computer abuse legislation is to make it a crime to "willfully, knowingly or maliciously" access or cause to be accessed a computer, com-

puter system or computer network. Certainly, this would apply to hackers. There is great concern in Congress that no legislation be enacted that would serve to punish the unauthorized person who inadvertently accesses a computer data base, or to unreasonably stifle creativity in young computer "whizzes." The use of the words "knowingly, willfully or maliciously" would appear to satisfy that concern. But, additional reservations were voiced with regard to definitions of the words "access" and even "computer." In an Indiana Law Review discussion by Michael Gemignani, titled "Computer Crime: The Law in '80", the question is raised as to whether the definition of "computer" in HB 1092 was so broad as to include electronic watches and some traffic control signals, while so narrow as to exclude some computers. Obviously, there are problems in writing high-tech law!

If the FBI had the investigative authority, how much computer abuse would be found? We're not sure. Of the types of crimes in which computers are involved, it appears that the greatest number are crimes committed using the computer as a means (certain frauds, embezzlement and the like, which can be prosecuted oftentimes under existing legislation) and the fewest reported involve attempted penetrations of a computer data base. But, in the absence of statistical records, there are great unknowns. Furthermore, inasmuch the potential losses from data base penetrations—in dollars and secrets—are so great, effective computer abuse legislation is considered vital.

The computer hacker is nothing if not interesting. It is possible to profile young hackers; they do fit a fairly common mold. Their usual techniques, too, can be catalogued and, therefore, defeated. The entry into the Los Alamos system has been discussed and the responsibility was frankly laid to some poor security measures coupled with a policy of making that system easily accessible to legitimate users. This is true to every penetration accomplished by the Milwaukee hackers. They were not so skilled; security was that easily defeated. And, those security defects were correctable.

The most useful technique of the accomplished hacker, however, is the "con." Making pretext telephone calls to legitimate system users has

provided many a hacker with a password. Raiding the garbage at night; looking for print-outs; accessing business space on a pretext; finding passwords users have "hidden"; even visiting bars near a facility after working hours in an effort to meet ADP personnel. All viable and successful techniques, all defeatable by a good security program. The hacker on the outside can be stopped. The hacker on the inside . . . that's another matter.

The hacker who works for an organization can be a major asset. His/her inquisitiveness, persistence and intelligence can be a vital part of a progressive program. But, what about the hacker who doesn't respect secrets—or authority? He, too, has access to the system. If there is a potential major problem from hackers, the hacker on the inside is it. Security officers must consider the possibility of establishing profiles for hiring purposes; separation of responsibilities is critical; a security staff with programming expertise "on board" will be a necessity; a constant review of programs and personnel is vital.

Hacking is typically an adolescent phenomenon—most grow out of the desire to indiscriminately prowl through another's property. As the number of hackers increases, however, without an observable mutual growth in ethics, the possibilities become increasingly worrisome.

DOE INITIATIVES IN TECHNOLOGY TRANSFER A HIGH TECH APPROACH

Robert R. Fredlund, Jr.
Director, Classification and Technical
Information Division
U.S. Department of Energy
Albuquerque Operations Office
Albuquerque, N.M.

Introduction and History

About nine months ago when Mike Lower first asked me to make this talk, he told me to please remember that the seminar would after all be in Las Vegas and, therefore, it was most important that I grab the attention of the audience right away, and hold it! As a matter of fact, he said it didn't really matter too much what I talked about as long as it would be interesting. He even spec-

cifically suggested that I try to arrange a couple of brand new jokes, since most of those in the audience would have heard all the ones that I have told before.

I advised Mike that, since I worked for the U.S. Department of Energy, which is a very professional, technical Government entity, naturally my talk would be of great substance; however, I would try to make it as interesting as possible, and would even include a couple of new jokes, if he would agree not to schedule my talk on the last day, as he has always done in the past. There was a pause at the other end of the phone; no doubt to give Mike time to cross all of his fingers and toes before he replied, "Don't worry, we'll put you on right in the middle of the seminar—perhaps on the second day. That way everybody will be there to hear your very interesting talk." "Incidentally," he asked, "what are you going to title your talk?" "I think I will title it something zippy like Technology Transfer—A DOE Perspective," I replied. "Oh," he said.

I should have known better. A couple of months ago Mike called me back and told me that due to "circumstances beyond his control," it would be really much better if he could move my talk to Friday. "Would I mind terribly?"

I reminded him that on Friday everybody leaves and that it would be nice if there were two or three people in the audience to hear my talk, after all the time I plan to spend on preparing it. "No problem," he said, "I have thought up a really snazzy title to your speech—a real grabber. We'll call it "DOE Initiatives and Technology Transfer—A High Tech Approach. That will really grab their attention! Just one more thing—we really need for all the speakers to provide a written text of their speech." Disaster! I was so upset by the prospect I forgot to protest being moved to Friday! Speaking from a written text is about as foreign to my nature as going on a cottage cheese diet would be to John Puckett! However, I have dutifully prepared such a text and I am now giving it to Mike Lower. Those of you who take the trouble to read it in your journal, however, will note that it bears very little resemblance to what I am going to talk to you about today, for the aforementioned reason.

In any event, in order to grab your attention as promised, I have titled my talk as Mike suggested

"DOE Initiatives and Technology Transfer—A High Tech Approach." However, I'm really going to talk to you about DOE perspectives and technology transfer, since, as I have said, almost everything we do in the DOE is by definition high tech.

The DOE Dilemma

The DOE is in a somewhat unique position in the Government, in that it is required by statute both to disseminate technology and to control aspects of the same type of technology. The principal statute governing DOE operations, the Atomic Energy Act is, in itself, somewhat internally inconsistent, in this regard. For example, in Section 141a, the Act requires the DOE to take appropriate measures to safeguard and prevent the unauthorized disclosure of Restricted Data, which is defined quite broadly as "all data concerning the design, manufacture, or utilization of atomic weapons, and the production of special nuclear material. . . ." Meanwhile, Section 141b of the Act requires that the DOE take appropriate measures to maximize the publication and dissemination of technology developed by the Department's research and development program to the maximum extent possible "so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information."

As if this weren't confusing enough, Sections 147 and 148 of the Act, which were enacted in 1980 and 1981, respectively, further require the Secretary to take appropriate measures to prohibit from unauthorized disclosure certain specified unclassified information concerning nuclear safeguards, security, and weapon and facility design.

To further complicate matters, Congress passed the Stevenson-Wydler Technology Innovation Act of 1980, which requires, inter alia, that the DOE spend one-half of one percent of its R&D budget to transfer technology.

As an additional complication in the lives of DOE Classification and Technical Information staff, the DOE is also subject of course to Executive Order 12356 and other "guidance," in the form of statutes, Executive Orders, etc., such as The Export Administration Act of 1979, The International Traffic and Arms Regulations, The Mutual

FIGURE 1

TECHNOLOGY TRANSFER THE DOE DILEMMA

- ATOMIC ENERGY ACT INTERNAL BALANCES
 - § 141 RESTRICTED DATA
 - § 141b ("MAXIMIZE TECHNICAL PUBLICATIONS")
 - §§ 147 & 148 (PROHIBIT "UNAUTHORIZED DISSEMINATION OF UCNM")
 - EO 12356 (NATURAL SECURITY INFORMATION)
 - STEVENSON-WYDLER TECHNOLOGY INNOVATION ACT OF 1980 (SPEND 1/2% OF R&D BUDGET TO TRANSFER TECHNOLOGY)
 - § OTHER GUIDANCE

Security Act of 1954, and The Commodity Control List, The Military Critical Technology List, etc., etc., etc.

A DOE Perspective

"Well," you might well ask, "what can the DOE possibly do to get a handle on that sort of a situation?" The answer is, it isn't easy. As a first step, we have taken steps to organize, to the extent possible, our philosophical approach toward a concept which identifies, to the extent possible, the form that the technology transfer may take. As you can see from the slide, there are a number of different ways of looking at the scope of the threat, including those indicated on the slide and others.

FIGURE 2

THE TECHNOLOGY TRANSFER THREAT CLASSIFICATION

- OVERHAULMENT
- CLASSIFICATION/CLASSIFICATION
- MATERIAL/CLASSIFICATION
- CRITICAL/CLASSIFICATION

Philosophically, because of the balancing required by the various statutes, Executive Orders, etc., which apply, it is necessary for the DOE to adopt a policy which allows DOE researchers and contractors to take maximum technical risks, while requiring minimum commercial risks by those commercial entities participating in the tech-

nology transfer program. At the same time, it is important that the DOE, in disseminating as much as possible of the valuable results of DOE research and development, maintain operational flexibility, and of course, in all cases, safeguard National Security. In order to best accomplish these objectives, we believe it is essential that results of all DOE supported Research and Development be carefully analyzed for technical content by personnel who are both technically competent in the subject matter and highly trained in the policy issues affecting classification, other categories of sensitive information, and technical information dissemination.

FIGURE 3

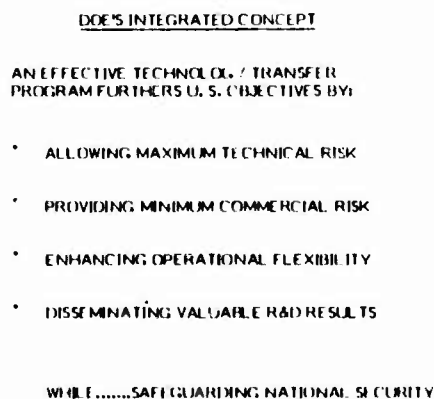
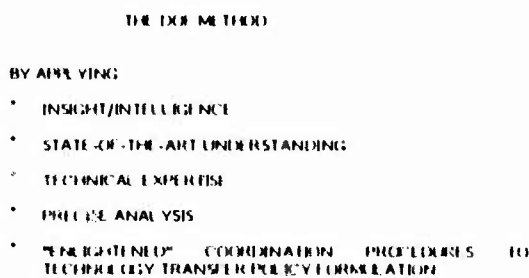


FIGURE 4

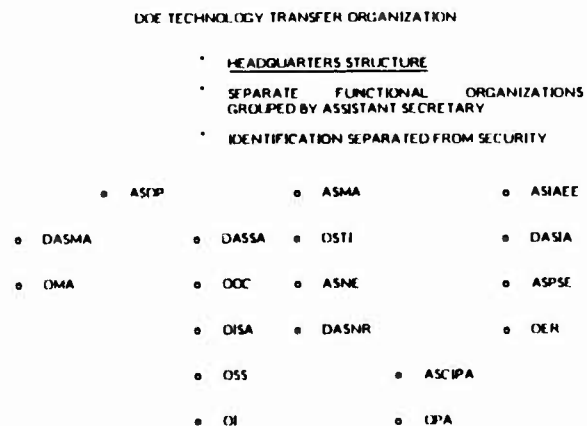


Developing a Coherent Policy—Organizational Initiatives

Organizationally, the DOE, like other Federal departments, has both a headquarters and field structure. As you might expect, headquarters entities are primarily responsible for development and coordination of broad policy issues and in maximizing intra-department consistency, both at headquarters and in the field, in the application

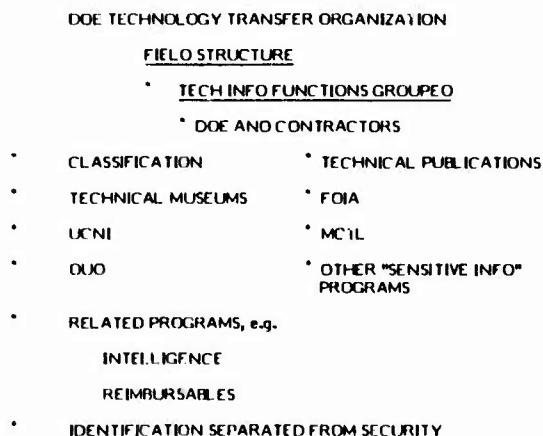
of policies developed. As you can see by the slide, because of the complexity in the many facets of technology transfer, there are an unusually large number of DOE headquarters entities involved in one or more aspects of the technology transfer program. Rather than bore you with a translation of all the acronyms shown, let me just point out one of the major organizational characteristics of all DOE information control programs, i.e., different organizations are responsible for formulating policies regarding the sensitivity, identification, and protection of information. This is true in both classified and unclassified areas.

FIGURE 5



The DOE field structure is similar, except for two factors. First, because of the nature of field activities and the much smaller resources available at each field office, functions are necessarily grouped. In many cases, in view of the required balancing which I mentioned above, functions relating to the protection and the dissemination of information are assigned to the same organizational entity. However, as I indicated was the case for headquarters, in almost all cases, functions relating to determining information sensitivity and identification, are separated from those involving information protection or other security issues.

Another somewhat unique aspect of DOE field operations is the close relationship between DOE Government field activities and DOE integrated contractors. Organization of Technology Transfer functions at the major integrated DOE contractors generally parallels quite closely with DOE organization in the sensitive information identi-

FIGURE 6

fication and control areas. Moreover, these major contractors generally operate, within their own organizations, direct extensions of the DOE. For example, in the DOE, much classification guidance is written by and for individual contractors by contractor personnel and contractor personnel are *required* to appoint an "appropriate" number of authorized classifiers, both derivative and original.

Thus, while DOE exercises policy control over its contractors, formulation of policy and procedures utilized for day-to-day operations or for application to information unique to a specific contractor is handled directly by the contractors with only general oversight by the DOE.

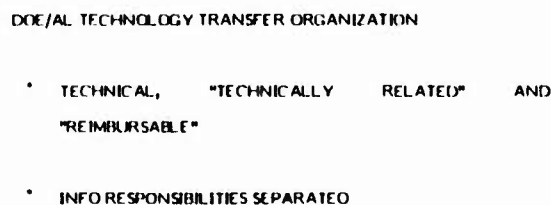
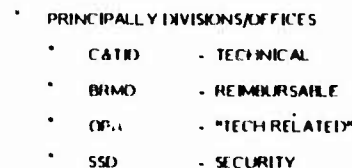
Albuquerque Operations Office (DOE/AL)— A DOE Microcosm

In order, hopefully, to clarify the organizational generalities discussed above, in the remainder of this talk I will address how these organizational concepts and information policies are applied at the DOE's largest field office, the Albuquerque Operations Office, of which, coincidentally, I am a part. As the slide alleges, Albuquerque Operations Office is in many respects, a DOE microcosm, and has responsibility for a wide range of DOE programs, including both nuclear weapons and nonweapons research and development, major activities such as the Waste Isolation Pilot Plant, and the Uranium Mill Tailing Remedial Action Project and a number of other major programs. As in a number of other DOE offices, those functions deal with technical information generated by DOE programs, "technically related infor-

mation," i.e., principally that disseminated directed to the public on a large scale through the media and otherwise; and information generated by DOE contractors for other Government agencies. This last category of information I have termed "reimbursable." The principal Albuquerque Operations Divisions and Offices responsible in these areas are addressed on the next slide. I have identified, as you can see, which Divisions are responsible for which information/functions.

FIGURE 7

ALBUQUERQUE OPERATIONS OFFICE (DOE/AL)
A DOE MICROCOSM

FIGURE 8**FIGURE 9**

Since I know it best, and Mike Lower promised you I would speak about "High Tech," and it covers the majority of Albuquerque Operations Technical Information activities, I would like to review with you in some detail the programs administered by the Classification and Technical Information Division (CTID). I have listed the Division's principal programs on the next slide. As you can see, they range from classification of the DOE's most sensitive nuclear weapons information to operation of one of the DOE's principal mechanisms for disseminating information about nuclear weapons directly to the public, i.e., the National Atomic Museum.

The scope of Albuquerque Operations activities is fairly broad, encompassing seven major integrated contractors in eight states and a host of smaller contractors involving both classified and unclassified technical information.

FIGURE 10

U. S. DEPARTMENT OF ENERGY
ALBUQUERQUE OPERATIONS OFFICE
CLASSIFICATION AND TECHNICAL INFORMATION DIVISION
(CTID)

- PROGRAMS
 - CLASSIFICATION
 - TECHNICAL PUBLICATIONS/SEMINARS, ETC.
 - NATIONAL ATOMIC MUSEUM
 - FREEDOM OF INFORMATION ACT (FOIA)
 - UNCLASSIFIED INFORMATION (UCNI) CONTROLLED NUCLEAR
 - MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL)
 - OFFICIAL USE ONLY (OUO) POLICY

FIGURE 11

SCOPE OF DOE/ALBUQUERQUE OPERATIONS

- 7 MAJOR "INTEGRATED" GOCON IN 8 STATES
- 35-50 MINOR CLASSIFIED CONTRACTORS
- 150-200 UNCLASSIFIED "TECHNICAL" CONTRACTORS

Classification Management

The DOE classification program is, as you would expect, responsible for the identification and categorization of the most sensitive information regarding both weapons and nonweapons programs generated by the DOE and its contractors. It's worth emphasizing again here, I believe, that even at, or perhaps *especially* at, the field level, the DOE emphasis in formulating policy regarding the identification and categorization of classified information is on technical analysis of the information, by technical people, who must have a state-of-the-art technical understanding of the subject matter, as well as remaining completely current regarding DOE and U.S. Government classification policy. Again, this is seen, within the DOE, as a function distinctly separate from security. On the next slide, I have shown the functional relationships between the various entities involved in the DOE classification program and in the various level of classification guides generated by the DOE, and its contractors, and utilized by DOE, its contractors and personnel from other Government agencies and contractors. As you can see, in this structure, the field office is

the link between the contractors and DOE headquarters. As such, the field office operates as sort of a buffer and "information filter" between these two somewhat disparate entities, while still allowing relatively direct and short lines of communications throughout the entire structure.

FIGURE 12

CLASSIFICATION MANAGEMENT

- THE IDENTIFICATION AND CATEGORIZATION OF SENSITIVE INFORMATION
 - KEYSTONE - TECHNICAL ANALYSIS BY TECHNICAL PEOPLE
 - SEPARATE FROM SECURITY

FIGURE 13

Classification Policy Development

- Contractors ↔ Field Office ↔ DOE/HQ ↔ other Agencies/Countries
- Guidance Hierarchy
 - Policy
 - Topical
 - Program
 - Local
- KEY-
 - Technical Competence
 - Programmatic Awareness
 } of Classification Staff

Similarly, in the formulation of classification guidance, local classification guidance for use by one or more contractors for a very specific project, is based on higher level guidance, prepared either in the field or at Headquarters as appropriate. In this regard, one important aspect in the development of DOE classification guidance is that field office and contractor input and evaluation is an essential part of the development of even the highest level of DOE classification and policy guidance.

Just a couple of final notes about classification program administration. The Albuquerque Operations Office maintains a small office at most of its major contractors. This office, which directly oversees the contract, commonly is termed an "Area Office."

Finally, each contractor, no matter how small, with a contract potentially involving classified information is required to have a technical person

responsible for operation of the classification program. At major contractors, this "Classification Officer" has a staff of as many as 5-10 additional technical personnel to assist in administering the classification program at the contractor. However, an unusual feature of the DOE program is that these "Classification" personnel, as well as those in the DOE area offices, do very little actual classifying of documents. This function is performed almost exclusively by technical programmatic personnel who have been appointed as either original or derivative authorized classifiers. Only in borderline, unique, or brand new areas are classification decisions regarding specific documents generally made by the Classification Office staff.

FIGURE 14

DOE ALBUQUERQUE
CLASSIFICATION PROGRAM ADMINISTRATION STRUCTURE

- * AREA OFFICES
- * CONTRACTOR CLASSIFICATION OFFICERS
- * AUTHORIZED CLASSIFIERS

Technical Information Program Management

The next major function of the Classification and Technical Information Division is almost the exact converse of the classification function, i.e., it is the purpose of the Technical Information Program to ensure that the results of all publicly funded research and development are recorded, preserved, published and disseminated to the maximum appropriate extent, so as to increase

FIGURE 15

TECHNICAL INFORMATION PROGRAM MANAGEMENT

TECHNICAL PURPOSES

- * ENSURE RECORDING, PRESERVATION, PUBLICATION AND APPROPRIATE DISSEMINATION OF RESULTS OF PUBLICLY FUNDED RESEARCH
- * IMPROVE TECHNICAL COMMUNICATIONS
 - * INTRAGOV
 - * INTERAGENCY
 - * WITH INDUSTRY
- * AVOID R&D REDUNDANCY

FIGURE 16

TECHNOLOGY TRANSFER ASPECTS OF THE TECHNICAL INFORMATION MANAGEMENT PROGRAM

- * DOUBLE-EDGED SWORD
- * ORGANIZATIONAL RELATIONSHIPS
 - * CLASSIFICATION/UCNI
 - * PUBLIC AFFAIRS
 - * AREA OFFICES
 - * CONTRACTORS

the national technical energy data base, avoid R&D redundancy and improve technical communications, both within and without the DOE. As indicated several times previously, accomplishments of these objectives require some delicate balancing, including close liaison with other organizations responsible for either controlling or promoting technology transfer.

The National Atomic Museum

One of my favorite aspects of the DOE technical information program is the National Atomic Museum which I like to categorize as a "unique national resource." As you can see from the slide, the National Atomic Museum has a number of functions and a variety of exhibits relating both to nuclear weapons and to non-weapons DOE activities. However, the focus of the Museum is, and always has been, the preservation of the history of nuclear weapons. It is the DOE's principal medium for communicating to the public the history of this program which continues to have such a major impact upon all of our lives. The Museum is not a public relations medium as such, but rather attempts to portray the history of the nuclear weapons program in as dispassionate and objective a fashion as possible. For those of you who might be interested in the Museum, I have brought along a few brochures describing the Museum and its activities. As you can see from the slide, the Museum is a major attraction in Albuquerque. It is not uncommon in an average month to have visitors from more than 45 states and a large number of foreign countries.

FIGURE 17

THE NATIONAL ATOMIC MUSEUM
"A UNIQUE NATIONAL RESOURCE"

FIGURE 18**NATIONAL ATOMIC MUSEUM FUNCTIONS AND ACTIVITIES**

- o CONTAINS NUMEROUS SCIENCE AND ENERGY EXHIBITS
- o CONTAINS THE WORLD'S MOST COMPLETE COLLECTION OF NUCLEAR WEAPON SHAPES
- o EXHIBITS THE MOST COMPREHENSIVE HISTORY OF THE DEVELOPMENT OF NUCLEAR WEAPONS
- o SERVES AS A MAJOR INTERNATIONAL TOURIST ATTRACTION (VISITORS FROM MORE THAN 100 COUNTRIES)
- o LIBRARY, PUBLIC DOCUMENT ROOM

FIGURE 19**ATTENDANCE AT THE NATIONAL ATOMIC MUSEUM**

o 1976	--	54,488
o 1977	--	61,647
o 1978	--	89,977
o 1979	--	92,579
o 1980	--	108,183
o 1981	--	116,186
o 1982	--	121,931
o 1983	--	125,100
o FROM ALL 50 STATES, THE DISTRICT OF COLUMBIA AND MORE THAN 100 FOREIGN COUNTRIES.		

The Freedom of Information Act

Another program which in the DOE is very much related to, although not coincident with, the technical information program, is the Freedom of Information Program. As you are no doubt aware, the Freedom of Information Act codifies the public's "right-to-know" what its government is doing. The original intent of the Act was to ensure that members of the public had an opportunity to become better informed regarding the activities of their government. However, our current experience, especially in the Albuquerque Operations Office, because of our highly technical nature, is that most Freedom of Information Act requests:

- Deal with Technical Information;
- Are frequently attempts at industrial espionage; or, seek to acquire "free" technology; and
- Are a means by which the requestor hopes to acquire classified information, in many cases involving the design of nuclear weapons.

FIGURE 20**THE FREEDOM OF INFORMATION ACT (FOIA)**

- CODIFIES THE PUBLIC'S "RIGHT TO KNOW"
- ORIGINAL INTENT - A BETTER INFORMED CITIZENRY
- CURRENT EXPERIENCE
 - INDUSTRIAL ESPIONAGE
 - ACQUISITION OF "FREE" TECHNOLOGY
 - CLASSIFIED INFO

Thus, it is extremely important that the DOE personnel responsible for administering the Freedom of Information Program are completely cognizant of DOE policy regarding the control of sensitive information and that they cooperate closely with those organizational entities responsible for controlling or promoting technology transfer. Hence, the inclusion of the Freedom of Information Program in the Classification and Technical Information Division.

Unclassified Controlled Nuclear Information (UCNI)

As mentioned earlier, in an attempt to further control the dissemination of sensitive unclassified information, the Congress in 1981 passed Atomic Energy Act Section 148, which authorizes disclosure controls for sensitive unclassified information in three general areas: nuclear facility design, security of nuclear facilities, and unclassified nuclear weapon design manufacture or utilization information. Those of you who attended last year's seminar will recall that Trisha Chico from the DOE's Office of Defense Programs, provided you with a comprehensive account of the origins of Section 148 and the DOE's plans for implementing it. In the next couple of slides, I'll summarize briefly for those of you who were not at the seminar last year and update for those of you who were here the current status of the DOE's program for the control of this sensitive unclassified information, which has been named "Unclassified Controlled Nuclear Information" or UCNI for short.

One of the things that we have attempted to do in the past year in the DOE with regard to UCNI is to define specifically, for the benefit especially of the general public, exactly to what types of information UCNI is meant to apply and to what types of information UCNI is not meant to apply.

FIGURE 21**UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)**

- * AEA SECTION 148 (1981)
- * AUTHORIZED DISCLOSURE CONTROLS FOR UNCLASSIFIED INFORMATION IN 3 AREAS:
 - * FACILITY DESIGN
 - * SECURITY
 - * NUCLEAR WEAPON DESIGN, MANUFACTURE OR UTILIZATION

In this regard, the DOE regulation implementing Section 148 of the Atomic Energy Act specifies that UCNI specifically applies only to Government information, i.e., any fact or concept which is either owned by the Government, produced by or for the Government or under Government control. Specifically, UCNI does not apply to non-Government information, i.e., information which does not fall within one of the aforementioned categories. To make the intended scope of UCNI even clearer, the regulation specifies certain prohibitions regarding the administration of UCNI, and also a number of areas of scientific and technical endeavor, types of records and certain technical programs to which UCNI specifically does not apply.

FIGURE 22**GOVERNMENT INFORMATION****ANY FACT OR CONCEPT—**

- OWNED BY THE GOVERNMENT
- PRODUCED BY OR FOR THE GOVERNMENT
- UNDER GOVERNMENT CONTROL

With regard to the prohibitions on the use of UCNI, assuming that the information or documents under consideration are in fact Government information or documents, prohibitions regarding the use of UCNI generally parallel those applied to classification. Two items which are somewhat unique to the UCNI environment are the prohibitions against identifying information or documents as UCNI in order to restrain competition or prevent or delay the release of information which is not in itself UCNI.

FIGURE 23**PROHIBITIONS**

- CONCEAL—
 - VIOLATIONS OF LAW
 - INEFFICIENCY
 - ADMINISTRATIVE ERROR
- PERSONAL OR ORGANIZATIONAL EMBARRASSMENT
- RESTRAIN COMPETITION
- PREVENT/DELAY RELEASE OF INFORMATION NOT UCNI

Among the exemptions, aside from the obvious exemptions listed on the first half of Figure 24, I believe it is worth noting that essentially all health and safety information which is not specifically required to be protected for reasons other than safety and health, as well as essentially all programmable or technical information concerning low level commercial radioactive waste shipments and the Waste Isolation Pilot Plant is specifically exempt from the scope of UCNI.

FIGURE 24**EXEMPTIONS**

- NON-GOVERNMENT INFORMATION
- NOT ATOMIC ENERGY DEFENSE PROGRAMS
- CLASSIFIED INFORMATION
- BASIC SCIENTIFIC INFORMATION
- EMPLOYEE SAFETY INFORMATION*

*WITH EXCEPTIONS

The next slide provides a conceptual diagram of the manner in which UCNI policy is formulated and disseminated to appropriate officials for application to specific documents. Generally speaking, the program and procedures outlined on the slide closely parallel those used for the DOE's classification program. The key point is that decisions regarding coverage or application of UCNI to areas of information are made at a

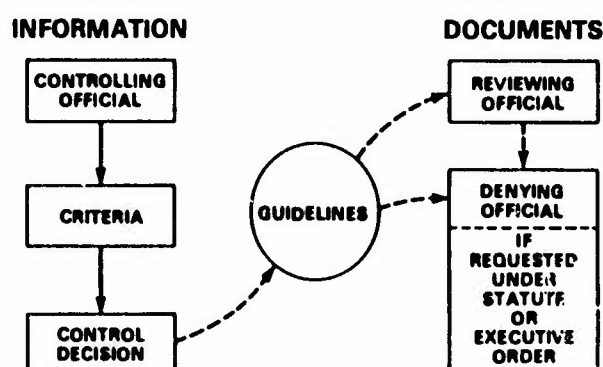
FIGURE 25
EXEMPTIONS

- **RADIATION EXPOSURE DATA**
– **PERSONAL HEALTH INFORMATION**
- **PUBLIC HEALTH AND SAFETY**
– **ENVIRONMENTAL INFORMATION***
- **LOW LEVEL/COMMERCIAL RADIOACTIVE**
WASTE SHIPMENTS
- **WIPP***

*WITH EXCEPTIONS

fairly high, centralized level and then disseminated widely to field activities for specific application in the context of local technical programs and documents. In this way, we intend to maximize, to the extent possible, consistency among various DOE and DOE contractor entities in the application of UCNI criteria.

FIGURE 26
AUTHORITIES



I have included the next couple of slides because they reflect a salutary, and somewhat unique approach to the identification and marking of sensitive information. As you will note on the slides, there are three separate markings which are authorized under appropriate circumstances. The marking displayed on Figure 27 is intended as a warning to personnel receiving Government information in the form of documents for a variety of purposes, that the information in the documents so received is within the scope of the information generally covered by Section 148. By

using this marking as a warning rather than as a definitive identification of information authoritatively identified as UCNI, it should be possible to provide the requisite degree of protection to a relatively large number of documents, while maintaining the centralized review procedures which are important in maximizing consistency of application.

FIGURE 27

MARKINGS

WHO MAY APPLY?

- **ANYONE**

WHEN?

- **PENDING REVIEW**
- **RETIREMENT**
- **OTHER**

NOT FOR PUBLIC
DISSEMINATION

 CONTAINS INFORMATION THAT
MAY BE SUBJECT TO SECTION
148 OF THE ATOMIC ENERGY ACT
OF 1954, AS AMENDED 42 USC
2160. REVIEW BY THE
DEPARTMENT OF ENERGY PRIOR
TO RELEASE IS REQUIRED.

The two markings illustrated on Figure 28 are alternative methods for definitely identifying information as UCNI. The first marking, which contains the maximum amount of descriptive information is intended for general applications. The second marking is an alternative for use, if for any reason, it is impracticable or inconsistent with the purpose of Section 148 to apply the more generalized language. In summary, it is hoped by allowing this flexibility in marking requirements, it will be possible efficiently to apply Atomic Energy Act Section 148 across the DOE and still retain

FIGURE 28

MARKINGS

WHO MAY APPLY?

- **REVIEWING OFFICIAL**

WHEN?

- **UPON POSITIVE**
REVIEW FOR UCNI

UNCLASSIFIED CONTROLLED NUCLEAR
INFORMATION NOT FOR PUBLIC
DISSEMINATION

 UNAUTHORIZED DISSEMINATION
SUBJECT TO CIVIL AND CRIMINAL
SANCTIONS UNDER SECTION 148 OF
THE ATOMIC ENERGY ACT OF 1954, AS
AMENDED 42 USC 2160.

OR

NOT FOR PUBLIC DISSEMINATION

 UNAUTHORIZED DISSEMINATION
SUBJECT TO CIVIL AND CRIMINAL
SANCTIONS UNDER 42 USC 2160.

the required degree of centralized control at DOE Headquarters.

Finally, Figure 29 describes the physical protection required for documents containing UCNI. In general, requirements for the protection of UCNI closely parallel those found within the Government for information which has been designated Official Use Only or a designation equivalent, or information which has been determined to be Proprietary by non-Government business entities. Thus, "prudent care" might be termed to be the criterion required for the protection of documents containing UCNI. In this regard, the requirements are sufficiently broad that a variety of conscientious, well-thought-out protection plans will be equally acceptable.

FIGURE 29 PHYSICAL PROTECTION

- SECURE CONTAINER
- LIMITED ACCESS AREA
- REPRODUCTION
- DESTRUCTION
- TRANSMISSION
 - MAIL
 - PERSONAL
 - TELEPHONE
- COMPUTER SYSTEMS

For those of you who are interested, I have brought with me a couple of publications by my Division which describe the history of, and current procedures concerning the handling of, UCNI by the DOE in general and the Albuquerque Operations Office and its contractors in particular. As you can see from the slides, the DOE's treatment of Unclassified Controlled Nuclear Information is roughly analogous to its program for the identification and control of classified information, albeit with somewhat less stringent specifications and controls, as is appropriate for information which is after all, by definition, unclassified.

Militarily Critical Technologies

Another interesting program which has been receiving a lot of attention lately is the Militarily

Critical Technologies List (MCTL). As you will recall, the MCTL is an attempt to list all of the technologies which would be of military significance to foreign countries. As interesting technology transfer aspect of the MCTL is that, unfortunately, the mere listing of all of the technologies which the United States considers to be of military significance provides a substantial amount of potentially useful intelligence information and might even, through the relationships of various technologies listed, act as a technology transfer medium.

FIGURE 30

- THE MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL)
- AN ATTEMPT TO IDENTIFY KEY MILITARY TECHNOLOGIES
 - PURPOSE
 - ID PREREQUISITE TO CONTROL
 - CLASSIFICATION ISSUE
 - STATUS

For this reason, it has been difficult for the agencies involved with the MCTL to agree upon an unclassified list. An unclassified list is of course desired, because unless the list can be made unclassified, it obviously can not be published to cleared commercial concerns, in order that they may be advised to control the export of technologies on the list.

Official Use Only (OUO) Information

Related to, but distinct from the DOE's UCNI program is the program for control of information designated for Office Use Only (OUO). Within the DOE, the OUO designation is used to refer to information which falls within one of the non-classification exemptions to the Freedom of Information Act. DOE policy with regard to FOIA exemptions, is of course, consistent with the intent of the Act, i.e., all of the exemptions are permissive. Therefore, if information which is designated as OUO is requested under the FOIA, it will be reviewed and considered for release to the public. Since, as mentioned before, many of our current FOIA requests relate to DOE technical contracts or programs, and in view of the relationship between OUO and the FOIA in the DOE, there are substantial potential technology transfer significance in much of the DOE's OUO information.

FIGURE 31

OFFICIAL USE ONLY (OUO) INFORMATION

- RELATIONSHIP TO:
 - FOIA
 - UCN
- DOE POLICY
- TECHNOLOGY TRANSFER SIGNIFICANCE

The Technology Transfer Threat—Real or Imagined?

As you can see, we have a multiplicity of programs in the DOE, and specifically at DOE field offices, concerned with the technology transfer threat. These programs are continuing to grow in significance as more and more people, both in government and industry, realize that the technology transfer threat is, in fact, real. As we have heard from a number of the previous speakers, it is not only a very real problem; it's a problem that is going to get harder and harder to solve as the United States and the world move into the post-industrial age, where technology is power, as well as being a vital ingredient in national wealth; and instantaneous communications between all points on the globe are a fact of life.

We've heard a number of interesting technology transfer "war stories" during the past couple of days, and DOE certainly has its share also. As you might expect, given the DOE's rather unusual requirements to both promote and control technology transfer, some of the DOE war stories are a little different.

For example not too long ago, Sandia Laboratories was engaged with several other countries in a major project to design commercially feasible solar energy systems. Naturally, since Sandia Laboratories was involved, the technology involved was very sophisticated and quite valuable. Because of this, a middle eastern country, not part of the project, requested access to design and performance data regarding the system. Since the data was quite valuable, the request was refused.

However, knowing that the information was unclassified, knowing a little about how the U.S. Freedom of Information Act operated, and being rather clever, the company from the middle eastern country formed a corporation in the United States and demanded that the DOE allow them

access to the technology under the Stevenson-Wydler Act, since they were now a U.S. company.

Since the Freedom of Information Act does not require requestors to be U.S. citizens, the company could conceivably have made a formal FOIA request, even without forming the U.S. corporation. However, they correctly perceived that the DOE would be much more likely to give the technology willingly to a U.S. corporation. Since the technology was unclassified, and since the dissemination of the technology was consistent with the purposes of the Stevenson-Wydler Act, the DOE was obliged to provide the technology to the U.S. corporation.

As might be expected in our position as Monday morning quarterbacks, the U.S. corporation gave the technology to their foreign parent company, which then used the information received to outbid all U.S. bidders for a recent major contract to build a solar energy system in the United States. Without the technology that they had received from Sandia via the DOE, they would not have been able to bid responsively on the contract, nor would they have been able to build the system.

A slightly different kind of war story that we run into from time to time in the DOE relates to nuclear weapon technologies that are not unique weapons, such as sophisticated electronics. Recently, a concern was raised that certain electronic technology which is used extensively in nuclear weapons, but which had been, in the main, determined to be unclassified some years ago, would be useful to possibly inimical countries or subnational groups for various military purposes. A meeting was held to discuss what could be done to perhaps identify the key components of the technology and then attempt to put some restrictions on these key bits of information.

After about two hours of meetings, with all of the experts analyzing the details of the technology from every conceivable angle, it was determined that enough key components of the technology had been disseminated that, as one member of the group put it, "no matter what we do, eventually the technology will still be available from Radio Shack!"

As you've heard all week, and as I have communicated today, the technology transfer control

problem is a knotty one indeed, and one with which we are just beginning to make a coordinated and enlightened attempt to deal. We certainly don't have all the answers yet and as you can see from the plethora of organizations just within the DOE concerned with technology transfer, it is going to take really enlightened communication and coordination both within government agencies and commercial companies, and especially between the government and its contractors if we are going to be really effective in dealing with the problem.

FIGURE 32

THE TECHNOLOGY TRANSFER THREAT
REAL OR IMAGINED?

At least, as you've seen from the presentations in the past several days, we are certainly becoming more alert to the problem and are beginning to understand the "real world" situation with regard to the ways in which valuable technology is inadvertently and unfortunately erroneously disseminated.

FIGURE 33

CAN WE MAKE TECHNOLOGY TRANSFER POLICY WORK?

KEY ELEMENTS

- ENLIGHTENED INTER/INTRA AGENCY COMMUNICATIONS/COORDINATION/SYNTHESIS
- "REAL WORLD" ANALYSIS

Thus, in summary, the bottom line is to be successful our technology transfer policy both within and without the government, must be clear, coherent, consistent, technically defensible, cognizant of what the "real world" situation is, both with regard to the technology and to legal and political arena in which it exists. Even though individual technology transfer issues may appear small, we cannot afford to allow ourselves the false sense of complacency exemplified by the cows that were wading through a Brazilian river which had a lot of funny looking small fish in it, each of which was only four to six inches long. One cow noticed this and remarked to the other cow, "I guess we don't need to worry about the fish in this river, they're only four inches long or so!"

FIGURE 34

THE BOTTOM LINE

TO BE SUCCESSFUL, POLICY MUST BE:

- CLEAR
- COHERENT
- CONSISTENT
- TECHNICALLY DEFENSIBLE
- COGNIZANT OF "REAL WORLD"

...GOVERNMENT-WIDE!

SAFEGUARDING ADVANCED CONCEPTS AND TECHNOLOGIES
(A Users Point of View)

Joseph R. Cacek, Jr.
Chief, Security Management
USAF Space Division
Los Angeles, CA

When first approached to speak, I really wondered what I had to offer to a group as experienced as this. I finally decided that since I had some experience as a user of the Industrial and Information Security Programs, I might have a little different perspective on the implementation of a DoD-wide program for controlling illicit technology transfer.

I. Parallels with the current Information/Industrial Security Programs:

a. DoD has apparently made a decision to springboard off of the Information/Industrial Security Programs. The current team approach (i.e., DIS, Industry, User Agencies) works.

b. Security Professionals (i.e., DIS, Industry, User Agencies) will have both great responsibilities and greater responsibilities under this program.

FIGURE 1

Parallels with the Industrial Security Program:

- Team Approach
- Implementing Directives
- "User Agency" Responsibilities
- Opportunities

II. Responsibilities:

- a. Establish a *Professional Image*.
- b. Educate both our Management/Command, and ourselves. ("5-pounds of security") (Get ourselves closer to the technologies. Get out from behind the desk!) Educate our organizations to the *reality* of the threat.
- c. Development and Documentation of specific control measures, which must be "do-able," affordable, and realistic.
- d. Management of those aspects under our control, and implementation of good security practices within our own organizations.

FIGURE 2

Responsibilities

- Establish an Image
- Educate
- Stipulate
- Control

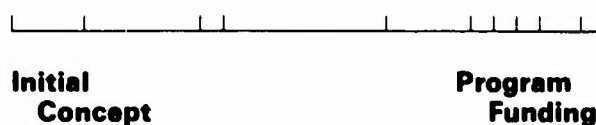
III. Development of Specific Control Techniques:

- a. All developmental efforts follow a relatively predictable pattern. By learning what this pattern is within our own organizations, we can choose the appropriate milestones for inserting security, OPSEC, and or Technology Transfer controls, without excessive impact on a programs progress.
- b. Within industry, and at least the USAF, the term "System Security Engineering" is coming into common usage.
- c. Failure to adopt a "Systems Engineering" approach will inevitably result in expensive secu-

urity "band-Aids" being applied to programs. In some cases, we have seen these retrofit security measures become so expensive that they have actually become financial tourniquets, killing a number of programs.

FIGURE 3

• Standard Timelines



- "System Security Engineering"
- Expensive Band-Aids vs Tourniquet

IV. Some Control Techniques:

a. Foreign Disclosures and Disseminations. Within our organization, processing of these types of actions, including approval of foreign visits, are done by my office. I have a trained killer on my staff who actually does this for us, and who has allowed us to maintain a manageable position from which we can stay informed and in control.

b. Having developed the contractual requirements which I mentioned earlier, we must then insure that they are contractually implemented in both prime and sub-contracts, funded as necessary, and made known to the DIS, in order that they may assist us in assuring compliance.

c. I've chosen for my last item a "favorite" of mine: releases at classified conferences and symposia. There is no question that this type of interaction and exchange between contractors and government is necessary. Conferences have been with us for years, and will continue so. We must start concerning ourselves, however, not only with the content and classification of a paper which one of our technical people may wish to present, but also with the type of forum (security environment) in which it is to be presented.

FIGURE 4

Control

- Foreign Disclosures
- Contractual Stipulations
- Conference Releases

FIGURE 5

Need-to-Know:

Authority for attending meeting is automatically granted to all active members of the XXX. Please include membership number with application and bring membership card for check-in verification. Non- XXX attendees must provide DOD approved Need-to-Know, signed by a Government Contracting Officer or his authorized representative.

FIGURE 6

"I, _____, certify that I currently possess a _____ level security clearance, and a Need-to-Know commensurate for the classified information to be presented at the _____ conference."

(Signed)

V. Conclusion:

- Opportunities

That says it all. As the DoD's Technology Transfer Control Program is implemented down to our level, those of us who have made the effort to educate ourselves, and to develop a professional and capable image will have many opportunities to excel. I myself have at least another two decades in this business. I am planning on making the most of it, and I am sure that you are too! Thank You.

DoD/INDUSTRY PANEL ON TECHNOLOGY TRANSFER

Gerald L. Berkin
Department of the Navy
Washington, D.C.

Good morning Ladies and Gentlemen. It's a privilege and an honor to have this opportunity to chair this distinguished DoD/Industry Panel on Technology Transfer for the National Classification Management Society. As panelists, we have Lt. Col. Joseph F. Murray representing the United States Army, Mr. David Whitman representing the United States Air Force in place of Mr. John McMann, and me, representing the United States Navy. For industry, we are privileged to also have with us today Mr. Dean Richardson of Texas Instruments Corporation.

Our assigned subject, technology transfer, is a fitting theme for this NCMS seminar, because it is a most timely topic, given the government's current efforts to stem the flow of militarily relevant technology to potential adversaries of the United States. And, given industry's and academia's apprehensions over control programs of this kind, then technology transfer is indeed a subject of topical and pressing interest to everyone in this room.

We are here as representatives of the Department of Defense and industry to briefly explain the military department and corporate view of the technology transfer problem, the proposed control mechanisms, and to address some of the problems which we are all expected to encounter in carrying out the government's objectives in this significant area. After the individual service and industry presentations, the panel will entertain questions from the floor; you may direct questions to a particular panelist or to the panel as a whole and I'll field the question to any panelist who believes he can handle it. Feel free to ask questions of the panelists after this period or at any other time; we are here, after all, to help you as best we can.

Now, whether the control of militarily relevant technology by the United States is a laudable objective or not is really beyond the province of this panel; we are here, basically, to describe the philosophy and the control mechanisms

employed, or to be employed by the military departments in support of the Department of Defense's Technology Transfer Control Program. Mr. Richardson will address industry and academia's perspective of this matter and his presentation should provide a balance of views with respect to the subject at hand.

As background for most of what has come about in the Defense Department, we must first talk about Section 1217 of the Department of Defense Appropriations Act of 1984 which amended Chapter 4 of Title 10, United States code, by adding a new Section 140C which basically reads as follows:

"Notwithstanding any other provision of law, the Secretary of Defense may withhold from public disclosure any technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be exported lawfully outside the United States without an approval, authorization, or license under the Export Administration Act of 1979 or the Arms Export Control Act."

Technical data with military or space application in the law's context means any blueprints, drawings, plans, instructions, computer software and documentation, or other technical information that can be used, or adopted for use, to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

The theory behind the amendment to Chapter 4, Title 10 U.S.C. is simply based on the fact that information, once publicly released is tantamount to having been exported. It then behooves the Department of Defense to withhold from public disclosure that information which would require licensing under the export control laws. This rather simplistic summation stems from what was, before Section 1217 of the 1984 Defense Appropriations Act, a glaring disparity between the pertinent statutes which required resolution. That is, the Secretary of Defense was not able, prior to Section 1217, to withhold unclassified technical information under the Freedom of Information Act, even if that same information would be licenseable under the export control laws. Assuming, of course, that the same information

could not be withheld under the then prevailing other FOIA exemptions. So, if an FOIA request resulted in the release of licenseable unclassified technical information, the licensing provisions of the export control laws would have been, in effect, circumvented—a clearly unsatisfactory state of affairs! The amended Chapter 4 of Title 10 has corrected this anomaly and the Department of Defense can now lawfully withhold from public disclosure certain unclassified technical information with military or space application.

It is necessary to point out, however, that the Department of Defense does not intend to deny access to export-controlled data to certified contractors who provide, or seek to provide, goods or services to the Department of Defense, or who will need such data to compete for foreign contracts in support of equipment or technology provided a foreign government by or with the approval of the U.S. government. There are other details pertaining to this policy which are contained in the appropriate DoD regulations.

It all comes down to, how does a free society protect itself without becoming a totalitarian society? Must we or should we help load the gun that is trained on us? Given the objective of stemming the flow of certain technological information to our adversaries, how are we to do so without causing a serious setback to our own technological efforts?

It would appear that the first thing which must be considered, once the objective is set, is to accept the fact that total and absolute control over information is an impossibility in and of itself. Even if it could be accomplished, the price we would have to pay would be unacceptable to free people. So, we must start by trying to reduce the flow of militarily relevant technology, rather than attempting to stop it completely.

Given the limited resources available for the control mechanisms, we had probably better concentrate on protecting truly critical technologies and information, because we just cannot cover the entire scientific and technological spectrum. From this, it follows that some sort of specific guidance will be forthcoming so that industry will know what can be publicly released and what cannot; in like fashion, government reviewers will also know what can and cannot be publicly released.

I cannot tell you the form such guidance will take; it may be in the format of a classification guide, a revised MCTL, or it may be in the form of an INFORMOGRAM or something like that. Be that as it may, before information can be selectively controlled, the selected information must be clearly identified so that the producers and the controllers "sing from the same sheet of music."

Above all, the system will depend in large measure on good faith. The good faith of the government to limit information control to only that information which warrants control under the law, and the good faith of industry and academia to support the government's efforts to safeguard militarily relevant technology in the nation's interest.

The objective has been set and we now must proceed with the work in good faith and give it a fair shake. Obfuscation by the government and evasions by the private sector won't help, but we can do what needs to be done if we all work together.

And now, I'd like to ask the individual panel members to make their brief presentations and we then will be happy to address your questions.

Joseph F. Murray
U.S. Army
Washington, D.C.

I am going to keep my formal remarks short. If you have any specific questions about the Army's Technology Transfer Program I will try to answer them during the question and answer period.

The basic assumption underlying the Army's T² Program is that it is important to control the flow of our critical technologies to our potential adversaries, particularly the Soviet Union, which relies heavily on the West for technology the Russians are unable to develop for themselves.

Our need to control the international flow of our technologies has presented us with a dilemma. While we must control the flow of technologies to our potential adversaries, it is equally important for military, political and economic reasons that we continue to share our technologies with friends and allies. Recent Army initiatives reflect our attempt to balance the paradoxical requirements of control and transfer.

The Army's T² efforts got their format start in December 1982 when the Chief of Staff, Army, made the Assistant Chief of Staff for Intelligence responsible for managing and coordinating all aspects of technology transfer. Two factors impacted heavily on ACSI's approach to T².

The first relates to a characteristic of T² itself. Simply stated, T² is more a concept than a function. Functional responsibilities related to T² are dispersed throughout the Army staff and its major commands. Any program that involves the actual or potential transfer of technology becomes by definition T².

The second factor, a lack of dedicated resources, reinforced the tendency toward a decentralized program caused by the alignment of functional responsibilities.

After a year and a half, the Army remains the most decentralized and least resourced of the services for T². With this as background I will now briefly run through current Army T² initiatives intended to result in consistent and rational T² decisions.

Major General Odom recently established the Technology Control Panel (TCP) to act as a coordinating mechanism for all T² issues. This Army level panel draws members from the Army staff and all major Army commands which play a role in T². The panel has representatives from the research, development and acquisition communities, as well as the intelligence and training communities. Two TCP initiatives are at the core of an effective Army T² Program, now and in the future.

The first initiative is a study which will propose a T² decision architecture for the Army. By architecture I simply mean a framework for how we in the Army decide when to recommend transfer and when to recommend control. This architecture, which is already being partially implemented, specifies responsibilities and procedures for staffing and reviewing T² issues. These issues can be anything involving the actual or potential transfer of technology. For example, foreign military sales, export license requests, data exchange agreements, MOU's and so on. In other words, any international program which

potentially involves the transfer of U.S. technology of importance to the Army.

I won't go into the architecture now, however, if you have any questions I will attempt to answer them during the question and answer period. What is important is what the architecture is intended to do.

Simply stated, we want to identify and assess the criticality of technology and systems or significance to the Army. Once we have identified a technology system or component as critical, we will evaluate its relative value to our adversaries. We then assess the risk of losing the technology to our adversaries if the specific transfer is approved. We base this assessment on the proposed recipient country's track record, as well as on their ability and willingness to protect our technology. After we have made these assessments we will determine if the potential military, political, technological, or economic gains of making a transfer are worth the risk. However, we currently lack a very important tool for totally and effectively implementing our architecture.

Providing this missing tool is the second major TCP initiative, we have initiated a program in the R&D community to specifically identify critical technologies embedded in our fielded, developmental, and future systems.

Once provided with this list we will be able to concentrate on controlling those technologies that are truly critical. We will be able to concentrate limited CI and OPSEC resources for the highest payoff. Systems not containing critical technology should quickly be approved for transfer; while those systems identified as containing critical technology will be transferred only after close scrutiny.

The U.S. Army Material Development and Readiness Command (DARCOM) is currently running a pilot project to validate the technology assessments. Once validated such assessments will be made on all Army systems on a priority basis.

In the future we anticipate making these assessments a requirement early in the R&D cycle. This will identify potential problem areas for the Army and industry. Alternative technologies for

key components can then be built into the development cycle, if appropriate.

The TCP, the decision architecture, and the Army list of systems and technologies critical to the Army, are the major on-going Army initiatives. We hope that they will yield a program for the Army which will produce timely, consistent and rational T² decisions regarding when it is in our interest to approve a transfer and when it is not.

In summary, we are learning and adjusting as we go along. T² is dynamic and changing. Hopefully, the Army's program which I have briefly outlined for you today is flexible and comprehensive enough to allow us to adjust to changing conditions. For us to make the most of our technological edge, we must delay its transfer to our adversaries, while sharing it to strengthen our allies and friends. How well we solve this dilemma is the T² challenge.

**David Whitman, DoD
speaking for
John McMann, USAF
Washington, D.C.**

Thank you for giving me the opportunity to address this group on the important issue of technology transfer.

The technology that the Soviets have acquired from the Western world has unquestionably played a major role in the modernization of both Soviet industry and military. We have all seen ample evidence of this fact reported through intelligence as well as the news media.

For decades the U.S. has had ample technological advantage and has not needed to be concerned by the flow of advanced technology out of this country. But today, as our technological lead becomes less great, we must recognize the technology responsible for that lead as the valuable and scarce national resource that it is.

We would certainly not allow a Soviet tanker to pull up to a U.S. dock and freely acquire crude oil, and yet this is precisely what they are doing to another valuable resource "our advanced technology."

Since the Soviets now have the numerical superiority for most weapon systems, we must protect our technological lead which partially compensates for our numerical inferiority.

The Air Force is committed to controlling the transfer of militarily critical technologies in order to maintain technological superiority of Air Force systems. This is our program goal. Notice that I say "control" the transfer of critical technologies rather than "stop" the transfer.

It would clearly be a mistake to overreact to the technology transfer problem by stopping all technology flow. The advanced state of the technology in this country is due in large part to the free flow of technical information within the domestic scientific and academic communities. A balanced view must be maintained. We need to balance our degree of restriction in accordance with the degree of sensitivity of the technology.

To achieve our program goal of controlling the transfer of militarily critical technologies, the Air Force is undertaking the following initiatives:

- To assure that Air Force technologies are adequately covered by the Militarily Critical Technologies List by providing active support to DoD's Militarily Critical Technologies Project.
- To identify for Air Force use, the most sensitive Air Force technologies that require the highest degree of control and restriction.

Both of these initiatives can be categorized as identification steps and are an absolute necessity to any reasonable control efforts.

We are establishing criteria to help us judge whether or not a given technology should be released by whatever means. It should be noted that technology transfer can occur by many means including but not limited to exports, conferences, publishing, foreign visitors, patents, and espionage. Use of the same criteria by those offices making release judgments for these various mechanisms will add necessary consistency to the overall process.

Consistency is a necessity. It makes no sense to restrict publication on radar absorbing mate-

rial and then allow an East German scientist to study at a U.S. university under the same professor that has an Air Force radar absorbing material contract. Likewise, it makes no sense for the Air Force to guard infrared detector technology if the Navy is giving it to the world. We must have consistency across both technology transfer mechanisms and organizational lines.

To give you an idea of what I mean by criteria, let me mention three criteria elements that should be considered in determining if release of a technology should be allowed. They are the military value or sensitivity of the technology, the ultimate destination of the transfer and the effectiveness of the technology transfer mechanism. For example, sale of a turn-key factory is a more effective mechanism than publishing a paper on the same subject. There are, of course, many other criteria elements that should be included, such as foreign availability, Soviet need, and state-of-the-art.

In addition to establishing technology release criteria, we are, for a limited number of technology areas, developing export and transfer policy guidelines to aid decision makers in that technology area. Our first such policy is for turbine engines and will be available shortly.

A few comments on the Air Force organization dealing with technology transfer follows. For each technology transfer mechanism from munitions sales to air shows, the Air Force already has a cognizant office in place. We do not intend to establish a vast new bureaucracy to deal with technology transfer. Rather, we intend to and are currently implementing an overlaying of technology transfer control responsibilities throughout those existing offices. This is established by a small network of concerned action officers interfacing with these Air Force offices, field commands, OSD, and other agencies. These action officers are developing new procedures and technology-oriented guidelines to assist Air Force offices in integrating technology transfer control into their existing activities.

The final major initiative I would like to discuss is our awareness effort. Because technology transfer decisions are made by the hundreds at scores of Air Force installations daily, it is mandatory that these Air Force field organizations be

made aware of the technology transfer threat and the new policies and procedures to deal with that threat. We have an active program to take this message to our field commands.

I would like to take an overview of the whole technology transfer issue, as related to classification. Over a period of years, we have come to realize that certain unclassified design and manufacturing know-how (as reflected by data) is providing an invaluable tool to the Soviet military machine. We categorize this know-how as our weapon system acquisition data. Because this body of acquisition data is so vast, classification is not a reasonable answer to protect the information. Therefore, we are searching for technology transfer controls to protect unclassified information that could properly be classified under Executive Order 12356.

Perhaps we should look more to classification to protect the small, most sensitive subset of design and manufacturing data, much of which is now treated as unclassified. And for less sensitive acquisition data, we should encourage proper use of the new DoD limited distribution markings as required by DoD Directive 5200.20. These markings do allow for limiting the distribution of unclassified critical technology information.

A brief word to industry before concluding. Do you know who your subcontractors are? Do you know how many communist-owned, U.S. chartered corporations are operating in this country? You should, the security of your nation is at stake.

In summary, I would like to leave you with a thought that I leave with Air Force field commands that I brief. Let us stop treating the release of technology as a default decision; let's all treat our critical technology as the valuable national resource that it is, and make its release a well thought out, conscious decision.

Dean C. Richardson
Manager, International Trade
Texas Instruments Incorporated
Dallas, Texas

Mr. President, Madam President Elect, Honored Guests, Ladies and Gentlemen, the only good

thing about appearing last is that maybe somebody will remember your message. Some of you may recall 20 years ago when some of us embarked collectively on a crusade to impact government policy on classification management and security guidance preparation. We did impact government classification management policy and today this country has a cost effective rational classification management program evolved by the dreaded military-industrial complex.

Well, I'm still crusading for logic, rational cost effective government, and today I hope I can enlist your aid in clarifying some concepts and definitions concerning technology and technology transfer.

I'm not going to talk about classification management or information security or security protection. I'm going to address technology and technology transfer—a matter of concern for your companies and the military departments being represented at this meeting.

What is high technology? Is there a low technology or how about a medium technology? Everybody talks about high technology even NCMS. It seems to be a very popular buzz phrase, which reminds me of phrases attributed to various decades. Remember the catch phrase of the 70's? The check is in the mail. And, of the 80's? It's only a cold sore?

We live in a society filled with little miracles. Most of these taken-for-granted miracles are the product of collective creativity. Some miracles trace their creation to the extraordinary work of individual inventors but most are products of collective efforts undertaken by major corporations at their own initiative.

The Wright Brothers were the individual inventors who reduced-to-practice the theory of manned flight, which in turn inspired the collective genius of countless others to create such miracles as: automatic flight path and automatic landing systems for airlines; cruise missile seekers and controls; and the technology that put Americans on the moon, sent probes into deep space and produced the first reusable space shuttle.

Alexander Graham Bell's telephone introduced

instant long range communication but the corporate creativity of thousands of people produced our miraculous communications system.

The invention of the integrated circuit opened the way for its ingenious application by engineers and scientists into useful products used every day in your home, office and vehicles as well as personal articles such as wrist watches with built in calculators and the hand held calculators with the computing capability previously available only from an assembly of large modular units. Also available are the unique learning calculators that speak, spell, teach math and translate languages; at a price everyone can afford.

All these things are miracles and all can be attributed to America's capacity for collective creativity. I'm sure that everybody here feels as I do that we Americans have an infinite capacity to innovate and continually advance our standard of living through technology so why worry about transferring technology?

The Soviet quest is one reason. Soviets have come to view the West as one great big shopping market for technology and have mounted a major effort to obtain it through espionage and other illegal means as well as legal means found in open societies such as the U.S. Freedom of Information Act. Just by asking the right questions, the Soviets are able to pull from U.S. government files, reams of technical data not otherwise available to the public, much of it only recently declassified. This Soviet effort is a massive well orchestrated effort, fashioned to:

- Significantly improve their weapon performance;
- Modernize Soviet industry;
- Save Soviet R&D rubles;
- Develop countermeasures to Western equipment.

And they have achieved a measure of success.

So what should we do? Assume a protectionist attitude and withdraw from the international market place for fear of losing our technology. Should we overreact by denying military products to our allies and withdraw from joint ventures? I don't believe that is the answer.

With the United States experiencing a balance of trade deficit of over \$60 billion in 1983, we can no longer afford the luxury of a negative export policy. It is important that the United States implement a coherent export control policy that directs events rather than reacting to them. A sound policy should be based on control of militarily significant technologies; and this control must be based on a precise definition of technology, a clear understanding of the mediums and mechanisms through which technology is transferred and an informed grasp of those technologies that most directly affect military systems.

Much of the confusion surrounding the issue of technology transfer is created by an inadequate or misdirected understanding of technology itself. Nationally we need to agree on the difference between high technology and advanced weapon capability. We need to grasp a clear understanding of the difference between science, technology and products.

People often speak of science and technology as though the terms were interchangeable; and of technology and know-how as though these were two different things; and it is not uncommon to see the meanings of science, technology and products used interchangeably.

The specific design and manufacturing know-how required to produce products is really the issue and it is of major importance. This is what technology is all about.

A clear distinction must be maintained between, science, technology and products. Science is the systematic pursuit of knowledge, while technology is the application of that knowledge to the production of specific goods and services. Technology is the design and manufacturing know-how required to produce goods. Technology is the specific know-how to define a product that fulfills a need and then to design and manufacture it, including the design and development of manufacturing processes and equipment! As opposed to technology, scientific information and data is exchanged around the world, adding to man's understanding; science alone does not provide a capability to produce goods. Therefore, products are the end results of technology but are not in themselves technology.

The difference between the export of products and technologies is that products satisfy short-term economic goals leaving the consuming country dependent on continuing imports; whereas the transfer of technology provides the consuming country with the capability to produce goods to meet both present and long term needs.

With these definitions as a frame of reference we can address the issue of technology transfer. How is it transferred? By the illegal means referred to earlier as the Soviet quest; and the legal means such as export licenses; memorandum of understanding executed between governments; the Freedom of Information Act; and the "two way street." The most effective mechanisms for transferring technology are turnkey factories, joint manufacturing ventures, proprietary manufacturing data exchange and patent licenses coupled with extensive teaching efforts.

On the other hand, hardware sales, trade exhibits, commercial literature, patent licensing without teaching efforts and reverse engineering of products are not very effective in transferring technology. The most common legal method of transferring technology results from a memorandum of understanding (MOU) executed between the U.S. government and selected Western allies, often referred to in diplomatic circles as "trans-Atlantic dialogue" but more commonly known as "the two-way street." This essentially means that when a foreign government buys our products, they expect to have part of the production accomplished in country and purchases of similar technology made in-country in an amount equal to a percent of the sale price of the contract. Industry refers to these requirements as offsets. For example, the following is the lead off in the preamble of a 12 page industrial protocol agreement which is a contract condition for the direct sale of military systems by Texas Instruments (TI) to a close NATO ally. The name of the country is left blank for obvious reasons; however, the agreement is representative. "The protocol is based on the cooperation principles laid down in the memorandum of understanding (MOU) signed 19 May 1978 between the government of _____ and the government of the United States of America concerning defense equipment cooperation."

"The purposes of this protocol are to establish

the framework for procurement from in-country manufacturers of products with technological level comparable to those manufactured by Texas Instruments Incorporated (TI) itself, as well as to establish the framework for an increased and longterm cooperation between in-country manufacturers and TI in the field of research and development." A little further on in Article 2, the protocol states "TI accepts the obligation to contribute to the realization of the general principles and aims of the agreement dated 19 May 1978 between the government of _____ and the government of the United States of America. TI makes the following compensation commitments: 2.1 TI agrees to a compensation of 100% of the total contract value as amended by contract modifications."

Needless to say, TI will make every effort to negotiate the 100% figure down to a reasonable level for our type of business which will still be difficult to satisfy.

This type of agreement has become associated with all large ticket items purchased by foreign countries. U.S. industry reluctantly is forced to accept this way of doing business internationally—if we want to stay in business.

U.S. trade deficits in 1983 exceeded \$60 billion, this means that the U.S. imported \$60 billion worth of products more than were exported. Some financial gurus expect the 1984 deficit to reach \$75 billion, unless there is a dramatic change in our export policies.

If U.S. industry becomes unable to compete with foreign firms for sophisticated international business we will be forced to concentrate on uncontrolled low technology commodity products in competition with emerging nations or, we could move our R&D and production to offshore industrialized countries whose export controls encourage international business. This would reduce U.S. employment and investment in U.S. facilities with a dramatic loss of tax base.

Industry needs export outlets to continually fuel our high technology industrial base after U.S. requirements have been satisfied.

In the past, most R&D efforts were funded by the government, and military application of tech-

nology preceded its commercial application. Today, electronic and aerospace technologies are developed by the private sector for commercial application long before these technologies are applied to weapon systems. For example, large scale integrated circuits developed through privately funded research appeared in consumer calculators, watches and appliance controls 7 to 10 years before they were used in weapon systems.

The development of commercial technologies with potential military applications—the so called dual use technologies—is accelerating. However, industry is not qualified to make determinations concerning the potential military application of a new process. Such determination must rest with officials knowledgeable with current and future weapon systems, with the advice and cooperation of industry. By the same measure, these same officials should not be so enthusiastic in applying export controls that they lose sight of the difference between technology and products and thus injure the competitive position of American industry unnecessarily.

Industry views current export controls:

- Overly broad and unilateral;
- Foreign availability is not considered during license review;
- Forces our free world trading partner to develop own capability;
- Removes incentive for U.S. industry to innovate; and
- Drives production overseas to U.S. subsidiaries and foreign prime contractors.

Richard N. Perle, the 42 year old Assistant Secretary of Defense for International Security Policy, has established a rather large DoD export control effort at a projected cost of \$10 million in 1984. This involves about 60 people in the Pentagon reviewing export license applications. So far this office has contributed to delaying export license processing by another 45 days. Because of his hard line on exports, Secretary Perle is also known in some circles as "The Prince of Darkness"—*Business Week*, 21 May 1984. Hopefully, Secretary Perle will become persuaded that unilateral control of military sales stifles the growth of our industrial base. What we really need is a more balanced approach between the security

and economic needs of the U.S.

Export controls must apply to the militarily critical technologies, and must be multilateral, must deal topically with foreign availability, must not treat allies like adversaries, must be enforced both in the U.S. and abroad and must recognize the role of exports in the world marketplace.

The facts of life are that technology transfer by whatever means is inevitable. Export controls only slow down the "catch-up" by the Soviets.

Here are some must do's to ensure U.S. technological lead time.

- Exercise strict export controls over critical technologies—not products.
- Remove controls over products available from foreign sources.
- Increase R&D spending in the U.S. by continuing the current 25% incremental R&D tax credit to encourage industry to allocate more dollars to their IR&D programs.
- Remove anti-trust barriers to joint ventures.
- Criminalize the counterfeiting of trademarks.
- Encourage commercial exploitation of new technologies.
- Further amend the Freedom of Information Act to restrict release of commercially sensitive data.

As a reminder to those of us engaged in international states and those who make policy decisions affecting export controls and ultimately international trade I would like to repeat President Reagan's Conventional Arms Sales and Transfer Policy dated July 8, 1981: "We will deal with the world as it is, rather than as we would like it to be." We will give high priority to requests from alliance partners and those nations with whom the U.S. has cooperative security arrangements.

- Degree the transfer responds to military threats confronting the recipient.
- Would the sale enhance recipients collective security efforts with U.S.?
- Would the sale promote mutual interests in countering externally supported aggression?

- Is transfer consistent with U.S. interests in maintaining regional stability?
- Is the sale compatible with requirements of U.S. forces?
- Can the receiving nation absorb financial and military support impact?
- Are possible detrimental effects of sale counter balanced by positive contributions to U.S. interests."

PART II

Workshops

This section contains reproductions of handouts of most of the workshop sessions. Some sessions did not have available materials and/or the data presented was not available. The handouts are mostly self explanatory and are furnished herein for information and use by Journal recipients.

WORKSHOP 1

CLASSIFIED DOCUMENT MARKING
PRACTICAL EXERCISE

Sheila K. Daigle

Defense

Investigative

Service

INSTRUCTIONS

Classified

Document Marking

1. The attached document consists of a FRONT COVER, a TITLE PAGE, INTERIOR PAGES, and a LAST PAGE. Indicate on these pages, where necessary, the proper classification. Indicate on these pages any other marking requirements, statements, etc., and on which page(s) they should be placed. NOTE: It is not necessary to write the full marking or statement. For example: do not write the name and address of the originator, draw a box or square and indicate what you would place in it.

2. A place has been indicated on each page of the document for the inserting of the proper classification. If you believe that the classification marks should be placed elsewhere on the page cross out the indicated places and place the markings where you believe they should be.

3. Bow-legs () have been placed by various portions of the document. Not all portions have bow-legs (). All portions have been numbered in the right hand column of the page. The classification of the information for the identified portions with or without bow-legs () is indicated on these instruction sheets. Please insert the correct classification for each of the portions indicated. If you believe that bow-legs () have been placed where they are not needed draw a line through the bow-legs (). If you feel that additional portions should be identified by bow-legs () with a classification, please insert them.

INDEX TO PORTION MARKINGS
(review paragraph 3 above before starting)

PORTION	PAGE 1	CLASSIFICATION
1		Unclassified
2		Unclassified
3		Unclassified
4		Confidential
5		Confidential
6		Secret
7		Unclassified
8		Unclassified
9		Unclassified
10 The contents of the table		Confidential
11		Unclassified
12		Unclassified

INDEX TO PORTION MARKING

PAGE 2

<u>PORTION</u>		<u>CLASSIFICATION</u>
1		Unclassified
2		Unclassified
3		Unclassified
4	The overall figure	Secret
5	NOTE: Numbers 5 thru 12 appear w/in the figure	Secret
6		Confidential
7		Confidential
8		Confidential
9		Unclassified
10		Secret
11		Unclassified
12		Unclassified
13		Confidential
14		Secret

PAGE 3

<u>PORTION</u>		<u>CLASSIFICATION</u>
1		Unclassified
2		Confidential
3		Unclassified
4		Confidential
5		Confidential
6		Confidential
7		Unclassified
8		Unclassified
9		Unclassified
10		Confidential
11	The overall figure	Unclassified
12		Confidential
13		Unclassified

INDEX TO PORTION MARKING

PAGE 4

<u>PORTION</u>	<u>CLASSIFICATION</u>
1	Unclassified
2	Unclassified
3	Confidential
4	Secret
5	Unclassified
6	Unclassified
7	Secret
8	Unclassified
9	Secret
10	Unclassified

PAGE 5

<u>PORTION</u>	<u>CLASSIFICATION</u>
1	Unclassified
2	Unclassified
3	Unclassified
4	Unclassified
5	Unclassified

PAGE 6

This is the last page of the document. Follow the instructions on the page.
No further portion identification is necessary.

Now complete the covers, title pages, etc.

FRONT COVER
(for classified
document marking
practical exercise)

T I T L E P A G E
(for classified
document marking
practical exercise)

(for training purposes only)

F I R S T P A G E
(for classified document
marking practical exercise.)

CHAPTER I
LASER DESIGNATORS ()

1. () The specification defines the Navy 5-inch guided projectile program and will be used to determine standards of performance. 2
- a. () Designators will be NdYag lasers such as the GLLD, ALLD, An/FQR-56 and M7LE. 3
1. () Wavelength will be 1.06425 microns. 4
2. () Power output will be 100 millijoules. 5
3. () Target spot size will be less than 1 inch at 0.5 km with a beam width of 0.01 mille radian. 6
- b. () Compatibility between systems will be constant. 7
2. () Tri-service codes will be used. Table I indicates the coding scheme for three (3) variable bandwidths. 8

() TABLE I

<u>BAND A</u>	<u>BAND B</u>	<u>BAND C</u>
100.1	101.1	234.5
100.2	101.2	234.6
100.3	101.3	234.7
100.4	101.4	234.8
100.5	101.5	234.9

() Tri Service Codes

3. () Among the performance standards for the 5-inch guided projectile are: 4 & 5
- a. Wavelength at 1.06425 microns.
- b. Power output at 100 millijoules.
4. () Among the performance standards for the 5-inch guided projectile are the wave length at 1.06425 microns and power output at 100 millijoules. 4 & 5
5. () This page has been an example of numbered paragraphs, sub-paragraphs using an alpha-numeric system. 12

(for training purposes only)

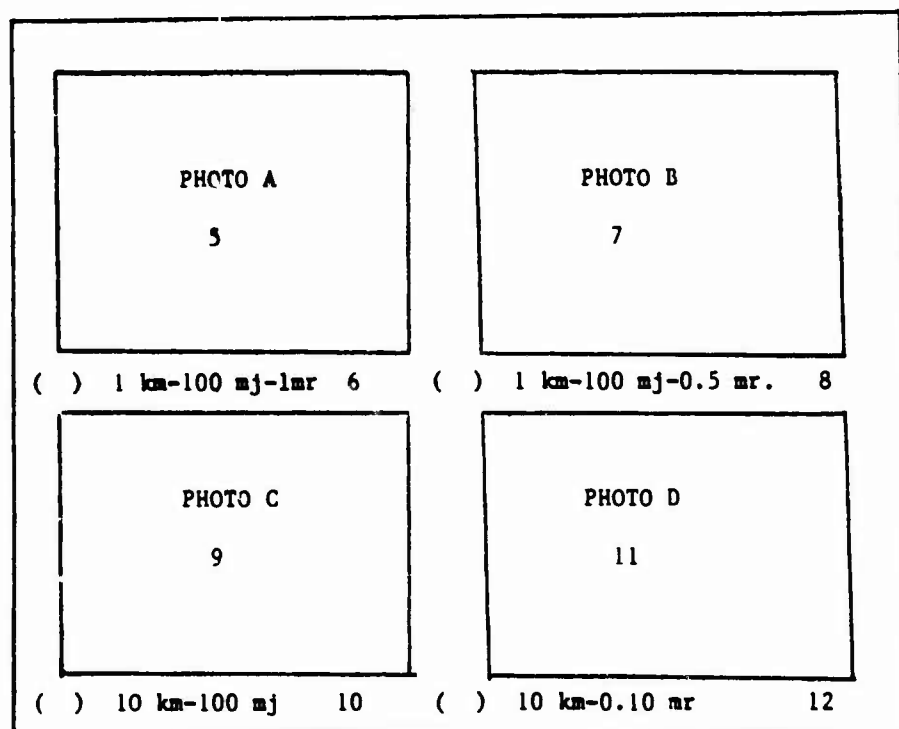
(for training purposes only)

3.0 () PHOTOGRAPHS ()

1 & 2

3.1 () Random samplings of laser designator spot density taken from field tests are shown in Figure 2.

3



4

Numbers
5 thru 12
appear in
Figure

() Figure 2. Spot Densities-100mj with Variable Radians

13

3.1.1 () Variables from 100 millijoules to 110 millijoules to the ratio of 0.01 milliradians to 1.0 radians creates a susceptibility to countermeasures in certain instances such as designator is in the high power mode and the pulse is continuous.

14

(for training purposes only)

(for training purposes only)

3.2 () Test Rules

3.2.1 () Test results from Bangladeesh field tests.

3.2.1.1 () Significant strength increases were discovered in the recent laser designator spot density tests due to the high thin atmosphere of the test range.

3.2.1.2 () These increases were due primarily to the following changes in the manufacturing techniques.

() • Signal modulation

() • Random jitter flutter angles

() • Clarity of doubling crystals

() • Pulse agility

3.3 () Signal analysis indicates an improved laser designator performance at all ranges.

3.3.1 () The constant flow of power from the stanisfrabus to the fortistat appears to be the basis for improvement when the power source is a cadmium tuleride battery, Figure 3.

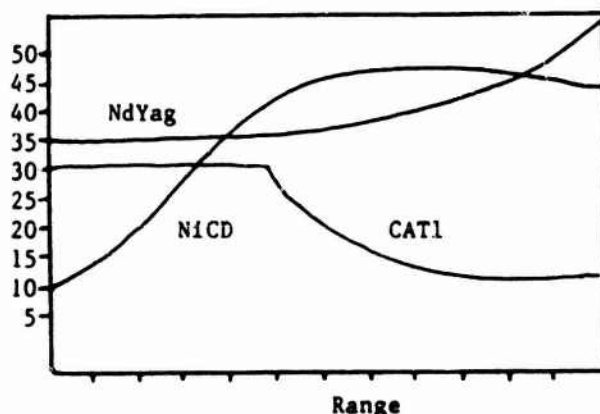


Figure 3. () Battery Power

4.0 () This has been an example of numeric paragraph numbering with both stand alone and topical paragraph headings.

(for training purposes only)

(for training purposes only)

CHAPTER II
ROTATING S. O. B.'S ()

- () Rotating side-orb blinders (SOB) present the modern version of unmitigated SOB's. Several generations of development were needed to improve unmitigated SOB's to rotating SOB's. 1
- () Rotating SOB's are also called revolving SOB's. The term R/SOB may be used interchangeably for either rotating or revolving SOB's. 2
- () The practical application of rear-end pressure expressed in foot-kicks (fk) per square inch was a major factor in the conversion of unmitigated SOB's to revolving SOB's. 3
- () Another item of the development program for rotating side-orb blinders was the use of the torsion spring clamp clip. (TSCC). As two are used in each R/SOB they are known as the tsk-tsk clips. 4
- () Installation of the tsk-tsk clips was initially accomplished by hand and resulted in many pinched fingers. 5
- () For obvious reasons this became known as the "damn-sam" operation. 6
- () To eliminate the "damn-sam" operation for the installation of the tsk-tsk clips, a modification was made to the bastion-retard (bas-tard) pin. This modification was the roughening of the external surfaces of the bas-tard to enable it to collect dirt particles. It was noted that the dirtier the bas-tard became there were significant changes in the unmitigated SOB's. Thus dirty bas-tards were a major contribution in the evolution of unmitigated SOB's to Rotating SOB's. 7
- () Individuals now bothered by unmitigated SOB's may convert them to rotating SOB's by use of the procedures expressed herein. 8
- () Apply rear-end pressure by means of foot-kicks. 9

(for training purposes only)

(for training purposes only)

- () Use tsk-tsk clips for the torsion spring clamp. 1
- () Be sure to use a dirty bas-tard. 2
- () Beware of the "damn-sam" operation. 3
- () Additional studies are being conducted to determine whether side-orb blinders (SOB's) may be further improved by the constant application of the rear-end foot kick pressures. 4
- () This has been an example of portioning by indentation only. 5

(for training purposes only)

JAWS III Part Classification Matrix

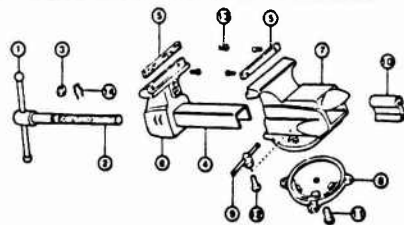


Fig. 3

There are a number of different ways in which the matrix concept has been adapted. Another example uses a matrix to include an entire mechanical assembly like a missile warhead, fictitiously titled "JAWS III". All the parts listed, 1 through 14, are organized in the table by material. The table then lists a series of classification questions, A through F, common to each part. The result is the matrix illustrated in Figure 3.

TOPIC NO.		1	2	3	4	5	6	7	8	9	10	11	12	13	14
SUB-TOPIC NAME		HANDLE	SCREW PIN	CLIP SPRING	TAIL GUIDE	JAW FACE	JAW PIN	JAW PIN	JAW PIN	NUT	SCREW PIN	CLIP SPRING	CLIP SPRING	CLIP SPRING	CLIP SPRING
A	PART	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U
B	SHAPE, ECHLED, UNECHELED	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U
C	WEIGHT OF PART	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U
D	MATERIAL	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U
E	FACT OF USE IN PART	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U
F	FACT OF USE IN NEW	U	CD	U	U	CD	CD	CD	CD	U	CD	U	U	U	U

Obviously, one has to premeditate the answers to each question for each part and then fill in the squares. Once this is done a new type of classification guide comes into being; one that shows a picture of each part, it's relative position in the assembly, what the part is made of and its classification relative to its size, weight, shape and association to other things.

Another adaption worth mentioning is the creation of a matrix guide based on an existing topical guide. The purpose of doing this is to enhance the guide for simplicity and clarification.

Anyone desiring an elaboration on the mechanism for creating simple classification matrices in their technical or administrative area, please contact Herman H. Teifeld, Classification Officer, Lawrence Livermore National Laboratory, P.O. Box 808, Livermore, California 94550.

(0319a)

WORKSHOP 3

Andrea Wraalstad

**Defense Investigative
Service**



PREPARATION OF
DD FORM 254

BRIEFING HANDOUT

CLASSIFICATION MANAGEMENT BRIEFING

Classified Procurement Steps

This information has been prepared to apply to a prime contract DD Form 254. The Industrial Security Regulation (ISR) references apply to the User Agency. Additional pertinent information is contained in Appendix D, ISR; Section VII, ISR; and Paragraph 2-116, ISR.

1. Determine security requirements for the proposed contract.
2. Determine clearance status of prospective contractor. Contact the Cognizant Security Office for verification of the facility security clearance and safeguarding capability, if required.
3. Develop classification guidance for RFQ, RFP, IFB.
4. Distribute DD Form 254 for these in accordance with para. 7-103, ISR.
5. The security classification requirements may be different for the pre-award phase than during performance. If may, therefore, be necessary to construct a specimen DD 254 which would be a part of the package as a specification on which the prospective contractor can base his cost estimates for performance. If the pre-award phase does not require access to classified information, Item 110, Remarks, should be annotated to indicate that pre-award access is not required and that the 254 reflects the access requirements for the contract to be awarded.
6. Upon selection of successful contractor, issue DD 254 for the contract. This will always be an original DD 254 even though one was issued during the solicitation stage.
7. Distribute DD 254 for the contract. (7-103a, ISR)
8. Review security requirements during the different stages of the contract; e.g., preaward, award, Research and Development, Production, etc. Issue a revised DD 254 as necessary. Review the security requirements at least biennially (7-104, ISR), upon final delivery of goods and services and on termination of the contract.
9. Transfer accountability of the residual documents to a follow-on contract or authorize retention of the documents and issue a Final DD Form 254. (7-106, ISR)
10. Encourage the contractor to assist in the preparation of the DD 254 whenever possible.

ITEMS 2, 3, 4, and 5 for RFP, RFQ, OR RFB. Check 2c, enter number in 3c, and due date in 4c; enter date in 5a.

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER <small>Prime contracts must be shown for all subcontracts</small>		4. DATE TO BE COMPLETED <small>(Estimated)</small>		5. THIS SPECIFICATION IS: <small>See "NOTE" below. If item 5 or 6 is "Y", also enter date for item 5.</small>	
a. PRIME CONTRACT		a. PRIME CONTRACT NUMBER		a.		b. ORIGINAL Complete date in all cases	
b. SUBCONTRACT (If so item 13 for subcontracting beyond second tier)		b. FIRST TIER SUBCONTRACT NO.		b.		c. REVISION NO. DATE	
c. REQUEST FOR BID REQUEST FOR PROPOSAL OR REQ FOR QUOTATION		c. IDENTIFICATION NUMBER N00014-83-R-0001		c. DUE DATE MAR 30, 1983		c. FINAL DATE	

ITEMS 2, 3, 4, and 5 for Prime Contract. Check 2a, enter number in 3a, estimated date of completion in 4a, and date in 5a.

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER <small>Prime contracts must be shown for all subcontracts</small>		4. DATE TO BE COMPLETED <small>(Estimated)</small>		5. THIS SPECIFICATION IS: <small>See "NOTE" below. If item 5 or 6 is "Y", also enter date for item 5.</small>	
a. PRIME CONTRACT		a. PRIME CONTRACT NUMBER N00014-83-C-0001		a. JUN 1986		b. ORIGINAL Complete date in all cases	
b. SUBCONTRACT (If so item 13 for subcontracting beyond second tier)		b. FIRST TIER SUBCONTRACT NO.		b.		c. REVISION NO. DATE	
c. REQUEST FOR BID REQUEST FOR PROPOSAL OR REQ FOR QUOTATION		c. IDENTIFICATION NUMBER		c. DUE DATE		c. FINAL DATE	

ITEMS 2, 3, 4, and 5 for Revision to Prime Contract. Check 2a, enter number in 3a, estimated date of completion in 4a, leave date of original in 5a (Date), check item 5b, show revision number and date of revision.

2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER <small>Prime contracts must be shown for all subcontracts</small>		4. DATE TO BE COMPLETED <small>(Estimated)</small>		5. THIS SPECIFICATION IS: <small>See "NOTE" below. If item 5 or 6 is "Y", also enter date for item 5.</small>	
a. PRIME CONTRACT		a. PRIME CONTRACT NUMBER N00014-83-C-0001		a. JUN 1986		b. ORIGINAL Complete date in all cases	
b. SUBCONTRACT (If so item 13 for subcontracting beyond second tier)		b. FIRST TIER SUBCONTRACT NO.		b.		c. REVISION NO. DATE	
c. REQUEST FOR BID REQUEST FOR PROPOSAL OR REQ FOR QUOTATION		c. IDENTIFICATION NUMBER		c. DUE DATE		c. FINAL DATE	

The date of the original DD 15- will appear unchanged on each revised and final DD 15-. Each time a revision is made, it will be given a revision number. The original is revision 0 and each revision thereafter is given a sequential number.

ITEM 6: This block pertains to follow-on prime contracts. It must be to the same prime contractor for the same item(s) or services, with no changes in the security classification guidance applicable to the contract. When these conditions exist, enter an X in the "Yes" box, and enter the number and completion date of the preceding contract in items 6a and 6b. In item 6c, enter an X in the "Is" box. In all other cases, enter an X in the "No" box. This is an important block because it authorizes the contractor to transfer accountability of classified material from the preceding contract to the current one. It eliminates the need for the contractor to request retention of the classified material until completion of the current contract.

6. Is this a follow-on contract? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If YES, complete the following:		
a. <u>N00014-82-C-0001</u>	b. <u>DEC 31, 1982</u>	c. Accountability for classified material on preceding contract
PRECEDING CONTRACT NUMBER	DATE COMPLETED	
<input checked="" type="checkbox"/> Is <input type="checkbox"/> Is not, transferred to this follow-on contract.		

ITEM 7: Enter the name and address of the prime contractor in Item 7a. The name and address in this item should be identical to that furnished by the Cognizant Security Office when the facility security clearance was verified. In Item 7b enter the Federal Supply Code (FSC) number of the facility. The Cognizant Security Office will provide this number at the time of verification of the facility security clearance. In Item 7c, enter the appropriate Cognizant Security Office for the prime contractor.

7a. Name Address & Zip Code of Prime Contractor	7b. FSC Number	7c. Name Address & Zip Code of Cognizant Security Office
ABC Corporation 123 Broad Street Boston, MA 02210	12345	Director of Industrial Security 495 Summer Street Boston, MA 02210
7d. Name Address & Zip Code of First Tier Subcontractor	7e. FSC Number	7f. Name Address & Zip Code of Cognizant Security Office
7g. Name Address & Zip Code of Second Tier Subcontractor	7h. FSC Number	7i. Name Address & Zip Code of Cognizant Security Office
activity associated with I/P, R/P or S/P *		
* When actual performance is not specified, indicate such other location as applicable.		

ITEM 10: Enter a description of the procurement in Item 10a. This may be material, studies, services, etc. The statement should be short, concise, and unclassified. Item 10b is the Department of Defense Activities Address Directory number. Item 10c indicates whether or not the procurement will require security measures that are additional to those normally required in the ISM, such as access to Sensitive Compartmented Information or other special access programs. Item 10d indicates whether part or all of the work performed on the contract will be inspected by an agency other than the Defense Investigative Service (DIS) Cognizant Security Office shown in Item 7c, as applicable. Affirmative answers in these Items require additional explanation in Item 15.

10a. General identification of the Procurement for which this specification applies		b. DoDAAD Number of Procuring Activity identified in Item 10d	
Project 254 Studies		N00014	
c. Are there additional security requirements established in accordance with paragraph 1-11.4 or 1-11.5 (SR)?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If YES, identify the pertinent contractual documents in Item 15	
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If YES, explain in Item 15 and identify specific areas or elements	

ITEMS 11a Through 11o: These items are marked "Yes" or "No" according to the requirements of each contract. An explanation of each item follows this illustration.

ACCESS REQUIREMENTS		YES	NO	ACCESS REQUIREMENTS (Continued)		YES	NO
a. Access to Classified Information Only as either Contractor/ Government activities.				Access to SENSITIVE COMPARTMENTED INFORMATION			
b. Receipt of classified documents or other material for reference only (no generation)				c. Access to other Special Access Program information Specify in Item 15			
c. Receipt and generation of classified documents or other material				Access to U.S. classified information outside the U.S. Panama Canal Zone Puerto Rico U.S. Possessions and Trust Territories			
d. Fabrication, Modification, Storage of classified hardware				e. Defense Documentation Center or Defense Information Analysis Center services not to be required			
e. Graphic arts services only				f. Classified ADP processing will be required			
f. Access to IPD information.				g. REMARKS			
g. Access to RESTRICTED DATA							
h. Access to classified COMSEC information.							
i. Cryptographic Access Authorization required							

ITEM 11. ACCESS REQUIREMENTS (Explanation of individual items)

11a. Access to Classified Information only at other contractor/government facilities. Note the word "only." If the YES box is marked for this item, items 11b through 11e plus 11m and 11n must be marked NO and the remaining items marked as required. The contractor will not be required to have any safeguarding capability at his facility if this item is marked YES.

11b. Receipt of classified documents or other material for reference only (no generation). Note the word "only." If the YES box is marked for this item, 11a, 11c through 11e and 11n must be marked NO and the remaining items marked as required. Contractor's safeguarding capability will be required.

11c. Receipt and generation of classified documents or other material. If the YES box is marked for this item, 11a, 11b, and 11e must be marked NO and the remaining items marked as required.

11d. Fabrication/Modification/Storage of classified hardware. If applicable, include as much information as possible (additional info can be added in Item 15) to indicate if Restricted or Closed Areas will be required. How much hardware is involved? How large? When does the hardware become unclassified?

11e. Graphic Arts Services only. Note the word "only." If the YES box is marked for this item, 11a through 11d must be marked NO and the remaining items marked as required. This type of contract would not require any specific classification guidance because the markings on the documents provided would be sufficient guidance for the contractor. Contractor's safeguarding capability will be required.

11f. Access to IPO information. This means International Pact Organizations such as NATO, CENTO, SALT Talks, etc.

11g. Access to RESTRICTED DATA. This item includes access to FORMERLY RESTRICTED DATA and CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) and is information developed and controlled under the Atomic Energy Act of 1954. Note this item would always be marked YES if access to CNWDI is required.

11h. Access to classified COMSEC information. This item pertains to communications security information. Special briefings are required and you should consult the COMSEC Supplement to the TSM for other requirements.

11i. Cryptographic Access Authorization required. This item no longer applies.

11j. Access to SENSITIVE COMPARTMENTED INFORMATION. If this information is involved, your activity will have a Special Security Officer who should be contacted prior to any contracting. Special security measures are required. Items 11c and possibly 11d would have also been answered in the affirmative. Additional information must be included in Item 15.

11k. Access to other Special Access Program information. These types of programs usually require additional security procedures or actions. These requirements are varied and may be different for each type of Special Access Program. Additional information must be included in Item 15. Items 10c and/or 10d may also apply for these programs.

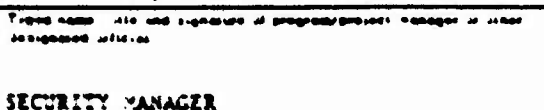
11l. Access to U.S. classified information outside the U.S., Panama Canal Zone, Puerto Rico, U.S. possessions and trust territories. Please indicate city and country of overseas performance in Item 15.

11m. Defense Documentation Center services may be requested. DDC is now the Defense Technical Information Center (DTIC). YES in this item will require that a DD Form 1540 and DD Form 1541 be prepared and processed by the contractor before he may request these services. The forms and other pertinent information are contained in Paragraph T, Appendix I of the ISM.

11n. Classified ADP processing will be involved. This item will be marked YES only if classified processing will be involved at the contractor's facility. It does not apply if the contract is for a maintenance service or when the contractor will be performing the work at a User Agency or another cleared facility. If this item is marked YES, the contractor will be required to prepare an ADP/SPP for his ADP operations and the system will require approval of the Cognizant Security Office in accordance with Section XIII, ISM.

11o. Remarks. This item may be used for any other pertinent information.

ITEM 12. Note that Item 12a is a statement of completeness and adequacy of the DD Form 254 that is being signed by the individual named in Item 12b. Item 12b contains the typed name, title and signature of the Program/Project or Security Manager. Item 12c contains the complete mailing address and telephone number of the individual named in Item 12b.

12. Refer all questions pertaining to contract security classification specification to the official named below. FORMALLY and ACQ items only. EMERGENCY , direct with contract manager and respond to ACQ item, prime contractor for subcontractors.	
a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.	
b. Typed name, title and signature of program/project manager or other designated official.	c. Mailing name, address, city, state, zip code, telephone number and office symbol.
SECURITY MANAGER 	Naval Research Laboratory Washington, D.C. 20375 (202) 767-1240
NOTE: Signature Specified on Item 12a is evidence of contractor's acceptance of classification specification. Revised and/or new specifications Item 12b and 12c are necessary for contractor to receive the requested classified information. Such action by contractor must be taken in accordance with the provisions of the instruction for users of ISM.	

ITEM 13: This item concerns the contractor's public release of any information under the contract. The contractor is responsible for obtaining the approval of the contracting officer for the prime contract.

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 3a and Appendix IX).

b. Proposed public releases shall be submitted for approval prior to release: ☐ Direct ☒ Through (Specify):

Commanding Officer, Naval Research Laboratory, Washington, D.C. 20375

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) * for review in accordance with paragraph 3d of the Industrial Security Manual.

* In the case of non-DoD User Agencies, see footnote, paragraph 3a, Industrial Security Manual.

ITEM 14: Items 14a and 14b specify the type of security classification guidance furnished for use in the performance of the contract. Item 14c indicates that the contract is a service-type contract. If Items 14a and/or 14b are used, Item 14c will not be used and vice versa. Item 14d is used for retention of classified material after the completion of the contract and requires approval of the contracting activity. Item 14e should read "Biennial review" instead of "Annual review" and is used to show the date the review is due.

14. Security Classification Specifications for this solicitation contract are identified below. ("X" applicable boxes) and supply attachments as required. Any narrative or classification guidance furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, the portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:

(I) Category of classification, (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (if applicable).

The official named in Item 12b is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☐ a. A completed narrative is (1) ☐ attached or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached or (2) ☐ transmitted under separate cover. List guide(s) under Item 3 or in an attachment by title, reference number and date.

☐ c. Service-type contract subcontract. Specify instructions in accordance with ISR/ISM, as appropriate.

☐ d. "X" only if this is a final specification and Item 5 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____

☐ e. Annual review of this DD Form 154 is required. If "X'd" provide date such review is due: _____

ITEM 15: Item 15 is the real purpose of the entire DD Form 254. This block is used to provide the contractor with the security classification guidance required for contract performance. The guidance will normally include one or more of the following:

- (1) Identification of security classification guides or extracts thereof which are furnished to the contractor or identification of the specific guides from which classification guidance may be obtained.
- (2) Narrative classification guidance which identifies the specific types of information to be classified and appropriate downgrading or declassification instructions. When classified hardware is part of the contract, identify the classified hardware and indicate when the hardware becomes classified.
- (3) Any special instructions and controls for handling, processing, storing, and transmission of the classified material.
- (4) Any explanatory comments or statements required for information or clarification of other items identified in the DD Form 254; e.g., 10c and d, 11 j, k and l.
- (5) When the contract is for certain types of services and Item 14c is marked, specific statements must appear in this Item. These statements are contained in paragraph 7-102, ISR.

This item may be expanded as necessary by adding additional pages as necessary.

15. Remarks. Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions.

ITEM 16: This item indicates the name and address of the approving official for the DD Form 254.

<p>16a. Contract Security Classification Specifications for Subcontractors issuing from this contract will be approved by the Office named in Item 16b below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.</p>	
<p>REQUIRED DISTRIBUTION:</p> <p><input type="checkbox"/> Prime Contractor (Item 7a) Paragraph 7-103, ISR</p> <p><input type="checkbox"/> Cognizant Security Office (Item 7c)</p> <p><input type="checkbox"/> Administrative Contracting Office (Item 16a)</p> <p><input type="checkbox"/> Quality Assurance Representative</p> <p><input type="checkbox"/> Subcontractor (Item 8a)</p> <p><input type="checkbox"/> Cognizant Security Office (Item 8c)</p> <p><input type="checkbox"/> Program/Project Manager (Item 12b)</p> <p><input type="checkbox"/> U. S. Activity Responsible for Overseas Security Administration</p> <p>ADDITIONAL DISTRIBUTION:</p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p>	<p>b. Typed name and title of approving official</p> <p>c. Signature</p> <p>d. Approving official's activity address and Zip Code</p> <p>e. Name, address and Zip Code of Administrative Contracting Office</p>

NOTE: The DD Form 254 is the only authorized means for providing classification guidance to the contractor for performance on a classified contract. It should be as specific as possible and it should include only that information which pertains to that specific contract. Encourage the contractor to assist in the preparation of the DD Form 254 and to provide comments on the guidance he has received. Work with the contractor to achieve guidance that you both understand and can use properly in order to protect the necessary information.

The CM Specialist for each Cognizant Security Office is listed below:

New England	Dick Maquire	(617) 451-4921	(AV) 955-4921
Mid-Atlantic	Ray Herot	(215) 271-4029	(AV) 484-4029
Capital	Andrea Wraalstad	(202) 325-8332	(AV) 321-8332
Mid-Western	Ruth Schafer	(216) 522-5344	(AV) 580-5344
Southwestern	Ralph Beeson	(314) 263-6581	(AV) 693-6581
Southeastern	Ted Skinner	(404) 429-6335	(AV) 697-6335
Northwestern	Sheila K. Daigle	(415) 561-5407	(AV) 586-5407
Pacific	Vacant	(213) 643-1084	(AV) 333-1084

TRAINING PURPOSES ONLY

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: <u>Secret</u>			
2. THIS SPECIFICATION IS FOR		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)		5. DATE TO BE COMPLETED (Estimated)		5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item e)	
X a. PRIME CONTRACT		b. PRIME CONTRACT NUMBER N00014-84-C-0001		30 June 1987		X c. ORIGINAL (Complete data in all cases) DATE 30 April 1984	
d. SUBCONTRACT (If item 3 is for subcontracting beyond second tier)		e. FIRST TIER SUBCONTRACT NO.				f. REVISED (supercedes all previous specifications) REVISION NO. DATE	
X g. REQUEST FOR BID, REQUEST FOR PROPOSAL, OR RFP FOR QUOTATION		h. IDENTIFICATION NUMBER N00014-84-R-0001		i. DUE DATE		j. FINAL DATE	
6. Is this a follow-on contract? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If YES, complete the following:							
a. PRECEDING CONTRACT NUMBER				b. DATE COMPLETED			
c. Accountability for classified material on preceding contract							
7. Name, Address & Zip Code of Prime Contractor: ABC Corporation 1112 Jefferson Davis Highway Alexandria, VA 22209							
8. Name, Address & Zip Code of Cognisam Security Office: Director of Industrial Security 11099 S. LaCienega Blvd. Los Angeles, CA 94129							
9. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IPB, RFP OR RFO							
10. General identification of the Document for which this specification applies: Technical Support Services							
11. Are there additional security requirements established in accordance with paragraph 1.14 of 1.15, ISM? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If YES, identify the pertinent contract and documents in Item 15.							
12. Are any elements of this contract outside the inspection responsibility of the Cognisam Security Office? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. If YES, explain in Item 15 and identify specific areas or elements.							
ACCESS REQUIREMENTS				ACCESS REQUIREMENTS (Continued)			
a. Access to Classified Information Only at other contractor/Government activities				1. Access to SENSITIVE COMPARTMENTED INFORMATION			
b. Receipt of classified documents or other material for reference only, no generation				2. Access to other Special Access Program Information (Specify in Item 15)			
c. Receipt and generation of classified documents or other material				3. Access to U. S. classified information outside the U. S. Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories			
d. Fabrication/Multiplication/Storage of classified hardware				4. Defense Documentation Center or Defense Information Analysis Center Services may be requested			
e. Graphic arts services only				5. Classified ADP processing will be involved			
f. Access to IPO information				6. REMARKS:			
g. Access to UNCLASSIFIED DATA							
h. Access to classified COMSEC information							
i. Cryptographic Access Authorization required							
13. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, the ACU from Item 10a) EMERGENCY, direct with written record of inquiry and response to ACO (from prime contractor for subcontracts).							
14. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.							
15. Typed name, title and signature of program/project manager or other designated official: Security Manager				16. Activity name, address, Zip Code, telephone number and office symbol: Naval Research Laboratory Washington, D.C. 20375 (202) 767-2240			
NOTE: Original Specification (from 3a) to authorize the contractor to mark classified information. Revised and Final Specifications (Items 3b and c) are authority for contractor to remove the required classified information. Such actions by contractor shall be taken in accordance with the provisions of the Industrial Security Manual.							

13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5a and Appendix (X)).

13b. Propose public releases shall be submitted for approval prior to release. (Direct) ☒ Through (Specify):

Commanding Officer, Naval Research Laboratory, Washington, D.C. 20375

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) * for review in accordance with paragraph 5a of the Industrial Security Manual.

* In the case of non-DoD User Agencies, see footnote, paragraph 5a, (Industrial Security Manual).

14. Security Classification Specifications for this solicitation/contract are identified below ("X" applicable box(es) and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:

(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (if applicable).

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☒ a. A completed narrative is (1) ☒ below, or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached, or (2) ☐ transmitted under separate cover. (List guides under Item 15 or in an attachment by title, reference number and date).

☒ c. Service-type contract/subcontract. (Specify instructions in accordance with ISN/ISM, as appropriate.).

☐ d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____.

☒ e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: 30 April 1985.

15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions).

1. Specifically designated contractor employees assigned to this contract will be required to hold Top Secret personnel security clearances for access to classified information.
2. Any classified information generated or received during performance of this contract will be classified, safeguarded and handled in accordance with the provisions of E.O. 12065, the DoD Industrial Security Manual, dated January, 1983, and OPNAVINST 5510.1F.
3. Contractor must submit all rough drafts of any contractor generated classified documentation to the program manager identified in Item 12b for a security review.

16. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, as by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.

REQUIRED DISTRIBUTION:

- ☒ Prime Contractor (Item 7a)
☒ Cognizant Security Office (Item 7c)
☒ Administrative Contracting Office (Item 16e)
☐ Quality Assurance Representative
☐ Subcontractor (Item 8a)
☐ Cognizant Security Office (Item 8r)
☐ Program/Project Manager (Item 12b)
☐ U. S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

1. Typed name and title of approving official

2. Signature

3. Approving official's activity address and Zip Code

4. Name, address and Zip Code of Administrative Contracting Office

DCASR
 605 Stewart Avenue
 Garden City, NJ 11530

*WORKSHOP 4**DOE Workshops***NCMS Training Seminar****Las Vegas, Nevada**

Two workshops were conducted at the NCMS Twentieth National Training Seminar by DOE employees Maria Barela, George Carnahan and Charles Demos. These workshops covered definitions and background of the classification levels and categories of information used by the DOE. There was discussion as to what is required of a subcontractor when they will be doing work

for DOE and already have a DOD interest. Discussions centered around a security plan and what is required in writing such a plan. Areas of document control, security education, security infractions, and visitor control were also discussed. Participation was solicited in a question/answer session. Copies of the slides used are enclosed along with handouts.

Restricted Data (RD)

All Data Concerning:

- (1) Design, Manufacture, or Utilization of Atomic Weapons;**
- (2) The Production of Special Nuclear Material; or**
- (3) The Use of Special Nuclear Material in the Production of Energy**

But Shall Not Include Data Declassified or Removed from the Restricted Data Category Pursuant to Section 142.

Formerly Restricted Data (FRD)

Information pertaining primarily to the Military Utilization of Nuclear Weapons which has been transferred or reclassified from the Restricted Data Category in accordance with Section 142(d) of the Atomic Energy Act (5)

National Security Information (NSI)

That category of information which is separate and distinct from the restricted data and formerly restricted data categories and which pertains to the National Defense and Foreign Relations (National Security) of the United States and has been classified in accordance with an Executive Order.

Areas a Subcontractor will need to Address when Preparing a Security Plan Include the Following:

- **Receiving Classified Documents**
- **Internal Control of Classified Documents**
- **Mailing Classified Documents**
- **Key Control**
- **Control of Combinations to Safes and Security Area Doors**
- **Access Control to the Security Area and Visitor Control**
- **Marking, Control, and Storage of Classified Matter**
- **Shipment Security**
- **Monitoring Procedures for the Security Area**

- Non-Duty Hours Security
- Security Education
- Personnel Security
- Violations
- Automatic (Electronics) Data Processing (ADP or EDP) System

Each Subcontractor Will Appoint a Security Officer and a Classified Document Custodian for their Facility. The Security Officer and the Classified Document Custodian Can Be the Same Person.

The Security Officer Has the Following Responsibilities for the DOE Security Program:

- Receiving and Disseminating DOE Security Instructions
- Enforcing Security Procedures
- Administering Security Orientations and Instructions
- Furnishing DOE with Requested Information Regarding the Facility Security Program
- Notifying DOE of Changes in Security Officer or Classified Document Custodian
- Obtaining DOE Approval Prior to Implementation of any Modification to Security Procedures or Safeguards Affecting Their Security Interests.

Security Infractions

The facility security officer is responsible for assuring that DOE security regulations are observed and that security infractions are held to an absolute minimum.

Assure that Necessary Action Is Taken to Preclude Recurrence.

Classified Document Control

- The Classified Document Custodian Will Be Responsible for Strict Accountability for Classified Documents Received or Generated.
- DOE Order 5635.1 Furnishes Information Concerning the Marking and Handling of Classified Documents.
- Employees with "Q" Access Authorizations May Have Access to Documents Containing Secret Restricted Data.
- Employees with "L" Access Authorizations May Have Access to Document Containing Confidential Restricted Data or Secret National Security Information.
- Mail Received Addressed to the Classified Mailing Address Will Be Delivered Unopened to the Security Officer.
- Custodians Must Assure that All Classified Documents Are Returned to Repository at the End of the Day.

- **When a Classified Document is Unaccounted For, Notify the Security Officer (Prime Contractor) in Writing Within 48 Hours Identifying the Document and the Circumstances Under Which the Document Became Unaccounted for.**

Security Education

The Facility Security Officer is Responsible for the Development and Maintenance of a Security Education Program.

SAMPLE SECURITY PLAN FOR FACILITIES

NAME OF COMPANY
& ADDRESS

SAMPLE FACILITY SECURITY PLAN
CONTRACT NUMBER

DATE (MO-YR)

The security procedures outlined in this plan have been accepted and authorized by the management of (name & address of company).

Date: _____ (Name, title & signature of
authorized company officials)

TABLE OF CONTENTS

SECTION	Page
I. Receiving Classified Documents	1
II. Internal Control of Classified Documents	2
III. Mailing Classified Documents	4
IV. Key Control	6
V. Control of Combinations to Safes and Security Area Doors	7
VI. Access Control to the Security Area & Visitor Control	8
VII. Marking, Control and Storage of Classified Matter	10
VIII. Shipment Security	11
IX. Monitoring Procedures for the Security Area	13
X. Non-Duty Hours Security	14
XI. Security Education	15
XII. Personnel Security	15
XIII. Violations	15
XIV. Automatic (Electronics) Data Processing (ADP or EDP) System	15
APPENDICES	
A. Security Area Characteristics and Floor Plan	16
B. Name of Company Q-Cleared Personnel	18
C. Security Area Control Sheets	20

I. Receiving Classified Documents

Classified documents mailed to (name of company) must be sent to the following DOE-approved mail channel address by registered mail:

Name and address of company
Attention: Name of authorized employees

No classified mail marked for (name of employees) will be opened by other than the addressee. Only specified Q-cleared employees approved by the responsible DOE Security representative will be authorized to handcarry classified documents between the post office, located at (address of post office) and (name and address of company). The company shall indicate in writing to the Post Office the names of the employees authorized to receive the registered mail. No mail addressed to either of the above locations will be left unattended.

The courier will:

- A. Travel directly between the two locations. (Using the most direct route and avoiding all unnecessary stops).
- B. Assure that envelopes and wrappers will:
 1. not be opened while enroute,
 2. be adequately sealed to prevent unauthorized access to the contents in transit.
- C. Assure that the locked briefcase used to transport classified documents is labeled with the name of the courier, his classified mailing address and telephone number
Note: Should the handcarrier fail to arrive within a reasonable time of his expected time of arrival, efforts will be made to determine the cause of delay. If the cause of delay cannot be determined immediately, notification will be made as soon as possible.
- D. Assure that all handcarries are properly logged.

Classified mail will be taken directly to the Security Supervisor or his alternate, who will immediately take the unopened package to the Security Area.

Classified mail will be opened in the Security Area only, where it will be logged in the Classified Document Log and placed in the safe. All envelopes will be carefully inspected, and any evidence of tampering will be immediately reported to the FBI, DOE. Upon opening the inner envelope, the enclosed "Receipt for Classified Information" will be dated, signed

and returned to the sender. Any discrepancy between the receipt and the contents will be immediately reported to the dispatching agency.

II. Internal Control of Classified Documents

Classified documents will be kept inside the Security Area at all times. Company (name) Q-cleared personnel must go to the Security Area to see the classified matter, and it may then be seen only on a need-to-know basis. Only classified documents, as prescribed by the contract, will be stored at company (name). During non-operating hours, classified documents will be stored inside locked GSA-approved 3-combination safes. All drawers will be secured (combination drawer last), dial spun at least four complete revolutions, and each drawer thumb-latch depressed while attempting to pull open the drawer.

The receipt of all classified documents will be entered into the Classified Document Log as follows:

- A. Control Number
- B. Date Received
- C. Classification
- D. Copy Number and Number of Copies
- E. Name of Person From Whom Documents Were Received
- F. Contract Number
- G. Unclassified Description
- H. Date Forwarded or Destroyed
- I. Person and Company Forwarded To
- J. Registration Number for Mailing
- K. Date Receipt for Classified Information Returned

Documents will be segregated according to issue number and classification.

Any documents removed from the safes during the day will be returned at the end of the working day and locked in the 3-combination safes. During the day, they will be constantly attended by a Q-cleared employee. When not in use or unattended, they will be returned to and locked in the safes.

All safes will be inventoried once each month to remove obsolete documents. Obsolete documents will be returned to, in accordance with the

procedures for mailing classified documents, and upon approval from the applicable Buyer.

No copies will be made of any classified documents without proper authorization. Additionally, no classified documents will be destroyed (e.g., shredded, etc.) at this site. Whenever a classified document cannot be accounted for instructions can be found on page 4, paragraph 6.g. in the Security Guide for Subcontractors, dated March 1981 (This will be revised in the near future).

III. Mailing Classified Documents

Classified mail will be *sent by registered mail only*. The document will be double wrapped, and the inner wrapper will be marked with the appropriate classification, top and bottom, front and back. An entry in the log book receipt and Receipt for Classified Information (RCI) will be made for the mailing and a "Receipt for Classified Information" will be sent with the package. The last copy of the RCI will be kept as a suspense copy. The entire package will be sent via registered mail.

Additionally, the following procedures will be followed:

- A. The RCI (which should be placed in the inner envelope) will identify the addressor, addressee, and contents by unclassified title.
- B. The inner envelope will bear (in addition to the classification markings previously mentioned) the return address and approved mailing address.
- C. If documents bearing different classifications are transmitted in the same envelope or wrapper, the markings shall be that of the highest level classified documents.
- D. The extra marking, category as well as level of classification, must be on the front of each inner envelope or wrapper.
- E. Appropriate measures will be taken to assure that:
 1. the security markings on the inner envelope cannot be seen through the outer envelope; and
 2. the contents of any classified documents transmitted cannot be seen through the inner envelope.
- F. The outer envelope will be addressed to the same address, and have the same return address, with no markings or notations to

reveal the classification or identification of its contents.

- G. All wrappers and envelopes will be tightly sealed.
- H. Only cleared personnel will take classified material to the post office.

IV. Key Control

All access to the Security Area will be by security-controlled keys (or combination locks). All alarm systems shall be activated and deactivated via security key locks. The following procedures will be followed.

- A. A limited number of Q-cleared employees of (name of company) will be issued keys or lock combinations to the Security Area. These employees will be initially limited to:

(name of authorized employees)
- B. All keys issued to employees will be numbered, and the employees will be required to sign a record book which will be maintained by the Security Supervisor.
- C. If an employee loses a key, it will be immediately reported to the Security Supervisor of (name of company.)
- D. If a key is lost, all locks operated by this key will be changed, and new keys will be issued to the appropriate employees.
- E. All extra keys will be stored in a locked safe under the control of the Security Supervisor, and records of each will be kept.
- F. Unauthorized reproduction of keys to the Security Area is *forbidden*.
- G. Keys will be inventoried at least annually.
- H. Keys and locks will be changed periodically (at least every five years), even though all keys are accounted for.
- I. If required, "Carry Home" keys will be limited to (name of authorized employees).

V. Control of Combinations to Safes and Security Area Doors

A limited number of (name of company) Q-cleared employees will have the combinations to the 3-way combination locks to the safe files or the combination locks on the Security Area doors if applicable. These employees initially will be:

(Names of authorized employees)

There will be no written record of the combinations retained (except in the DOE approved

security safes in the Security Area) by (name of company) employees.

A list shall be posted on the outside of the combination drawers of the safe files, listing all persons who may have access to the classified matter therein (name, address, and phone number).

All combinations and access codes shall be changed:

- A. Upon termination of an employee who is in possession of a combination, or
- B. At least once a year, or
- C. If a security compromise occurs, or is suspected.
- D. After outside maintenance.

VI. Access Control to the Security Area & Visitor Control

Q-cleared (name of company) employees shall be permitted access into the Security Area provided their name appears on the access list. The access list shall be posted inside the Security Area. Classified matter will be seen or discussed only on a need-to-know basis. Access will initially be limited to (name of authorized employees). If appropriate, authorized employees will wear company ID badges at all times.

The Security Area is monitored on a 24 hour basis by (explain system, if appropriate). At all times when the Security Area is unoccupied, the alarm system shall be activated by the last employee present.

Visits by DOE Q-cleared persons who require access to any classified information in the Security Area are approved *ONLY* by a DOE-277 form, "Request for Visit or Access Approval" which may be signed by a designated DOE/ALO Security Representative.

A list of persons whose DOE-277 forms are current will be posted at the main entrance door of the Security Area. All visitors requiring access to classified information will sign the visitor's register.

The security officer or designated alternate may inspect packages, boxes, containers, briefcases, etc. entering the security area. No prohibited articles (firearms, explosives, incendiary devices,

cameras, copying or reproduction devices, recording or transmitting devices) will be taken into the Security Area without proper authorization. A notice to this effect is posted at the entrance to the Security Area.

Visits to the Security Area by uncleared persons shall always be discouraged. If the visit is determined to be absolutely necessary, the Security Supervisor shall:

- A. Assure that the visitor wears a distinctive badge indicating his uncleared status.
- B. Assure that the uncleared visitor is prevented from viewing or obtaining access to classified information or classified material.
- C. Assure that all possible contacts are aware of the visitor's uncleared status.
- D. Assure that the visitor and the assigned escort understand that the visitor shall remain under the escort's physical control and direction at all times the visitor is in the Security Area.

In an emergency situation, when it is necessary that an uncleared person (such as maintenance personnel) be admitted to the Security Area, the area will be subject to prior inspection by the (name of company) Security Supervisor to assure that all classified matter has been properly stored to prevent unauthorized access.

All uncleared persons (also Q-cleared persons who are not employees and name of company) will be logged into and out the Security Area.

Detailed instructions on other aspects of visitor control are found on pages 15-16 of the Security Guide for Subcontractors.

VII. Marking, Control and Storage of Classified Material

All classified material must be identified by level of classification (Secret and Confidential) as well as category (Restricted Data, National Security Information). In addition, records must be kept on all classified material which indicate location of material and the employee responsible for the material.

- A. While not in actual use, classified matter (documents or material) must be constantly attended by an appropriately Q-cleared

employee or stored in a locked repository which has been specifically approved for such storage by the responsible DOE Security representative. Should operating requirements dictate the use of additional or substitute repositories, contact the Supervisor, Security Systems Division for approval.

- B. A monitor sheet containing spaces for initialing by the locker and monitor shall be posted on each repository containing classified matter. This sheet shall be initialed at the end of each workday by the person who has locked the repository, and except when not feasible, by one other person who has physically checked the lock, locked door or drawer, and all exposed drawers to ensure that the repository is properly secured.

VIII. Shipment Security

- A. Prior to each classified shipment of material, security notification, which includes date, protective service, weight, waybill number, number of containers, and estimated time of arrival, must be furnished to the recipient.
- B. For subcontractors authorized to ship classified material, the approved shipping address for _____ is:
Also list contractor company shipping address (if material is involved).
- C. The notification channel is:
- D. The approved classified mailing address for is:
- E. Packages containing classified material will be banded in at least two dimensions with steel strapping and secured with distinctive DOE ALO seals. A notched type banding will be used. The DOE ALO security seals will be obtained from: _____ prior to use. These seals will be protected to prevent use by unauthorized persons. Used seals will be mutilated to prevent reuse.
- F. Packages or containers of classified material, unless prohibited by health considerations, will have included a card or other notice which will immediately alert receiving personnel of the appropriate classification of the material.
- G. Shipping containers shall be inspected immediately upon arrival. Breakage of the container, seal, banding, or any evidence of tampering will be reported immediately.

IX. Monitoring Procedures for the Security Area

Q-cleared employees of (name of company) are appointed as monitors of the Security Area on a rotation basis.

The monitor's duties will be:

- A. To limit access of the Security Area to authorized personnel only.
- B. To ensure that the doors are locked at all times.
- C. To check the work areas at the end of the day to ensure that all classified materials and documents are properly stored and safeguarded.
- D. To store all classified materials at the close of the normal work day in approved storage locations and to assure that all documents are placed in proper repositories and that they are locked.
- E. To appoint a responsible Q-cleared employee to monitor the work area at the end of the "overtime" period in the event (name of company) employees are working hours other than normal. The overtime monitor will then become responsible for completing the monitor check sheet for that day.

The monitor will be the last person to leave the area and at this time will secure the doors.

The monitor will also check off and initial the monitor's check sheet each day, and initial the monitor sheet on the safes in the Security Area. The monitor check sheet will be maintained and appropriate entries made to assure the security of the area.

The monitor will turn any alarm switches on after signing the monitor's sheet. Indication that the system is active is provided on the alarm panel. The Security Area will be continuously monitored by (explain system, if appropriate).

As security is the responsibility of all individuals, each individual will be responsible for refraining from discussing classified information outside the Security Area, or with uncleared persons, or Q-cleared persons not having a need-to-know, while on the phone; and assuring that one's own work area is checked each evening.

X. Non-Duty Hours Security

The Security Area will be locked at all times during non-duty hours. The door and walls will

be built to specifications to bar forced entry. Access to the Security Area itself will be limited and controlled (explain non-duty security patrol frequency and procedure).

The Security Area will be continuously monitored (explain system). All alarm lines are supervised. This system permits continuous monitoring of the Security Area during non-duty hours. Q-cleared employees access the Security Area by (explain your method such as via a push-button combination lock on the door and a key-operated switch to deactivate the alarm system).

In case of an alarm during non-duty hours, (explain procedure and authorized employees to be contacted).

In the case of a break in, the FBI (list appropriate telephone numbers) will be notified immediately by the employee who responds to the emergency call.

XI. Security Education

See pages 7-10, Security Guide for Subcontractors, for details.

XII. Personnel Security

See pages 10-14 of the Security Guide for Subcontractors for information.

XIII. Violations

See pages 5-7 of the Security Guide for Subcontractors for information.

XIV. Automatic (Electronics) Data Processing (ADP or EDP) System

(If appropriate). An ADP (EDP) Security plan for classified operations on the (name/model of automatic data processing system or word processor) will be submitted in a separate document.

Appendix A Security Area Characteristics and Floor Plan

(Name of company) is located at (address).

Examples of the detailed physical security features are as follows:

Office space is maintained on three levels of the building. The vault room is situated on the lowest level. (Insert sketches or drawings of the surrounding area as well as of the office or plant facility, if appropriate).

A separate room 12' long and 7' wide located on the lower level is designated as the "Security Area." One wall, which is an exterior building wall, is constructed of concrete block. The remaining three walls are constructed of dry wall on solid wood studding. The floor is a solid concrete slab and the 7'4" high ceiling is a 6" drop ceiling suspended below solid wood planking. Access to this room is through a locked 1¾" solid wood door. The Security Area door lock is a push button combination lock.

Access to the Security Area is electronically monitored by magnetic door switch (ADEMCO Control #1022) and an infrared intrusion detector (RAYTEK, BISPY Series 82). This alarm system is activated and deactivated via a key lock and is monitored with self checking supervisory circuitry which alarm if tampered with. In case of power failure, the battery back-up power supply will continue operating for 12 hours.

The Security Area is monitored by (explain system, if appropriate).

Indicate in the event of an alarm, the alarm company calls a designated Q-cleared company employee(s) and both go to the facility to determine the cause of the alarm. If required, contact the local FBI office.

Appendix B (Name of Company) Q-Cleared Personnel

The following (company) Q-cleared personnel who will have access to the Security Area are:

<i>Names</i>	<i>Home Phone Numbers</i>
--------------	---------------------------

VISITOR REGISTER

[illegible]

(ALL VISITORS REQUIRING ACCESS TO CLASSIFIED MATERIAL MUST SIGN THIS REGISTER)

REPOSITORY INITIAL SHEET

NOTE:

This sheet is to be
initiated for both the
"1st check" and the
"2nd check" when
the repository is
secured at the end of
each day. Initiating
affirms that the
repository to which
this sheet is affixed
is securely locked.

GA 8003-A (11-77)

	MONTH:		MONTH:		MONTH:	
	1st check By:	2nd check By:	1st check By:	2nd check By:	1st check By:	2nd check By:
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						

24

MONITOR CHECK SHEET _____ 19 _

Date	Safe Locked	Access Door Locked	Alarm On	Initial	Overtime Monitor Assignment
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					

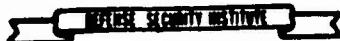
WORKSHOP 5

**Derivative Classification in Accordance
with a Security Classification Guide**
Joseph A. Grau



DEFENSE SECURITY INSTITUTE
Defense General Supply Center
Richmond, Virginia 23297

24 April 1984



PRACTICAL EXERCISE

SUBJECT: Derivative classification in accordance with a security classification guide.

EXERCISE TASKS: Portion mark a security classification guide (SCG). Use the SCG to determine markings for portions of a report. Mark pages of both documents. Determine applicable associated markings for the report.

TEACHING POINTS: (1) Classification markings on portions of documents must be based on the classification of information they contain or reveal. (2) Portion marking requires careful attention to what can be deduced from the portion, a clear understanding of the SCG's instructions, and logical thinking. It is not a purely "mechanical" process.

MATERIALS: HO 1, Security Classification Guide; HO 2, Report; Solution Sheet.

SUGGESTIONS FOR PRESENTATION: Distribute the handouts to the audience and allow time for them to mark HO 1. Then discuss the solution to this part of the exercise. Recommend the following points be noted:

- (1) The fact that marking of subjects and titles is often overlooked.
- (2) Need to mark each portion (including lead-in paragraphs) on their own merits. (Can vary based on organization policy.)
- (3) Absence of identification of the classification source and declassification instructions. (Suggest the instructor, after discussing the solution, ask if anything is missing on the SCG. When absence of these items is noted, explain they will be added by the "front office" when the SCG is approved.)

Allow time for marking HO 2, then discuss the solution. Recommend the following points be discussed:

- (1) Caution and logical analysis required to make sure nothing "falls through a crack" (paras 1 and 32).
- (2) The need for a clear understanding of the SCG's instructions and terminology ("durability" (para 7) and "effectiveness of destruction means" (para 17)).
- (3) Need to consider each portion on its own merits and in context (para 18).
- (4) Need to review entire SCG before use. Several sections can apply to one portion (para 21).
- (5) Method of identifying the classification source and determining declassification instructions. Note particularly that the date of the SCG is given and the declassification instruction is "OADR".

NOTES: "The Three Little Pigs" has been used for several years as a security training exercise. This version has been heavily revised from an exercise which bore no identification of the preparing agency. All materiel is UNCLASSIFIED.

SOLUTION SHEET: "Operation TRIPLE SWINE"

Security Classification Guide (HO 1):

Item 1d is S; items 1e and 2c are C; all other items and the title are U. Items are classified because they reveal the information they designate as classified, i.e., "the fact that" Page is marked SECRET top and bottom.

"Final Report: Operation TRIPLE SWINE" (HO 2):

Para 1: C [item 1b of the SCG] Note that the little pigs had the same mother. Later each is referred to as "he" and "him," so they must be brothers.

Paras 2, 3: U

Para 4: C [1e]

Paras 5, 6: U

Para 7: C [3c]

Paras 8, 9: U

Para 10: C [3c]

Para 11: C [3a(3)]

Para 12: C [3a(3), 3c]

Para 13: C [2c]

Para 14: U

Para 15: S [1d]

Para 16: C [2f]

Para 17: S [2f, 2g]

Para 18: U Since we know that the wolf blew the house down, we might think that his being out of breath would reveal how he destroyed the house. But he might have been out of breath because of any strenuous activity (e.g., using a sledge hammer. The paragraph really says nothing about the method of house destruction (or even that the house was destroyed), and is U.

Para 19: C [1b]

Para 20: S [1d]

Para 21: S [2f, 2g]

Para 22: C [1b, 3a(3)]

Para 23: C [1e, 3a(3)]

Para 24: C [2f]

Para 25: S [2f, 2g, 3c]

Para 26: U

Paras 27, 28, 29: C [1e]

Para 30: C [2c]

Para 31: C [1e, 2c]

Para 32: C [1e] If the pig could trick the wolf many times, he must be smart.

Para 33: C [3a(3)]

Para 34: C [1e]

Para 35: C [1b, 3a(3), 3c]

The title of the report is U. Both pages must be marked SECRET top and bottom.

Classification source and declassification instructions should read:

CLASSIFIED BY Operation TRIPLE SWINE SCG, 2 Aug 82

DECLASSIFY ON Originating Agency's Determination Required

ADDENDUM

Subsection 1-601, DoD 5200.1-R states that "persons who apply . . . derivative classification markings shall . . . verify the information's current level of classification as far as practicable before applying the markings. . . ." In many cases, the best way to do this is to consult the appropriate security classification guide (SCG). In addition, use of an SCG will almost always permit more precise and accurate derivative classification than use of source documents alone. This is easily demonstrated by adding an additional short task to the basic practical exercise, perhaps -- if time is constrained -- as a replacement for the section of the exercise involving portion marking of the SCG itself.

Students should be provided the following paragraph and instructed to consider it as a section of a source document they will use to derivatively classify a small portion of the "Final Report: Operation TRIPLE SWINE":

(S) Shortly after the three little pigs moved into their newly finished houses, a wolf demanded entrance to the straw house, crying, "Little pig, little pig, let me come in!" The pig, terrified to have a hungry wolf at the door, replied, "Not by the hair on my chinny-chin-chin!"

Point out that all the information found in paragraphs 13, 14 and 15 of the report is contained in this paragraph. Instruct the students to mark the appropriate classifications for the three paragraphs in the report, using this paragraph as source guidance. You might suggest the markings be placed above the parentheses so they can later be compared with markings based on the SCG. Then proceed with the rest of the exercise.

After the solution to the exercise has been discussed, ask the students to compare the markings on paragraphs 13, 14 and 15 based on the source paragraph with those based on the SCG. Without verification by means of the SCG or receipt of more specific guidance from the classifier of the source paragraph, all three paragraphs in the report would be marked Secret. Use of the SCG allows accurate marking, discriminating among the Secret, Confidential and Unclassified information.

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

Final Report: Operation TRIPLE SWINE ()

1. () Once upon a time three little pigs left their mother's home and went out into the world.
2. () One was a lively little pig who liked to dance.
3. () One was a happy little pig who liked to sing.
4. () One was a smart little pig who remembered what a wolf's real motives were.
5. () Soon the little pigs met a peddler hauling straw.
6. () The first little pig said, "Please sir, give me some straw so I can build a house."
7. () The peddler gave him some straw, and the little pig built his house; but straw is flimsy, so the house was not sturdy.
8. () The second little pig waited until a peddler hauling sticks came along.
9. () "Please sir," he said, "give me some sticks so I can build a wooden house."
10. () The peddler gave him some sticks, and the second little pig built a house. But some of the sticks came loose and the new little house almost tumbled down.
11. () The third little pig waited until a peddler hauling bricks came along. Then he said, "Please sir, give me some bricks so I can build a house." The peddler gave him the bricks.
12. () The third little pig built a strong brick house. It has a thick door and a big chimney.
13. () The three little pigs had just finished their houses and moved in, when along came a hungry wolf.
14. () The wolf stopped at the door of the straw house and called, "Little pig, little pig, let me come in!"
15. () "Not by the hair on my chinny-chin-chin!" cried the little pig.
16. () "I'll huff," roared the wolf, "and I'll puff and I'll blow your house in!"
17. () He huffed and he puffed and he did blow the straw house in.
18. () But the wolf was out of breath, and the little pig was able to scamper away to the door of the wooden house.
19. () The second little pig opened the door and let his brother in.

CLASSIFIED BY _____

DECLASSIFY ON _____

HO 2

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

20. () The wolf went to the wooden house and called, "Little pig, little pig, let me come in!" "Not by the hair on my chinny-chin-chin!" cried the little pig.

21. () "Then I'll huff and I'll puff and I'll blow your house in!" roared the wolf. He huffed and he puffed and he did blow the stick house in.

22. () Once again, though, the wolf was out of breath, and the two little pigs scurried to the door of the brick house. The third little pig opened the door and let his brothers in.

23. () The wolf rushed to the brick house and called, "Little pig, little pig, let me come in!" "No way!" replied the shrewd little pig.

24. () "I'll huff and I'll puff and I'll blow your house in!" roared the wolf.

25. () The wolf puffed and puffed and huffed and huffed, but he could not blow in the sturdy brick house. At last he gave up.

26. () "Come with me tomorrow morning at eight o'clock," he called, "and I'll show you Mr. Smith's fine turnip field."

27. () The next morning the smart little pig got up at five o'clock, went to Mr. Smith's field, pulled up some turnips, and skipped back home again before the wolf arrived.

28. () So another day the wolf came to the house again and invited the smart pig to go to the fair the following morning.

29. () The next morning the smart little pig got up early, went to the fair, and saw all the sights. While there, he bought a butter churn.

30. () He was on his way home when he saw the wolf coming toward him. The little pig hopped into his churn and rolled right past the frightened wolf, who had never seen a butter churn before.

31. () The next day the wolf came to the house. He told about the round thing that had frightened him. "Oh," laughed the smart little pig, "that was me rolling in my butter churn."

32. () The wolf gnashed his sharp teeth in anger. "You have tricked me many times, but you will never trick me again, little pig!" he roared. "I'm coming down the chimney and will eat you!"

33. () Quickly the wolf scrambled up on the roof of the brick house and made his way to the chimney.

34. () The smart little pig ran to the fireplace and whisked the lid off a pot of steaming water. When the wolf tumbled in, the little pig popped the lid in place -- and that was the end of the wolf.

35. () The three little brother pigs danced around the room. Then they settled down and lived happily ever after in the strong brick house with the thick door and big chimney.

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

Operation TRIPLE SWINE
Security Classification Guide ()
2 August 1983

1. () Pigs
 - a. () Number of pigs U
 - b. () Relationship of pigs C DECL 12 Feb 2000
 - c. () Fact that pigs are little U
 - d. () Fact of hair on chin S DECL 12 Feb 1991
 - e. () Fact that some pigs are smart C DECL 12 Feb 1991
 - f. () Other information U
2. () Wolf
 - a. () Existence of wolf U
 - b. () Size of wolf U
 - c. () Fact that wolf can be frightened C DECL 12 Feb 1991
 - d. () Intent to capture pigs U
 - e. () Motivation of wolf C DECL OADR
 - f. () Means of house destruction C DECL 12 Feb 1991
 - g. () Effectiveness of destruction means S DECL OADR
 - h. () Other information U
3. () Construction of houses
 - a. () Construction material used by:
 - (1) () Pig #1 U
 - (2) () Pig #2 U
 - (3) () Pig #3 C DECL 12 Feb 1991
 - b. () Sources of building materials U*
 - c. () Durability of houses C DECL OADR

*Unless type of material used by Pig #3 is revealed.

FOR TRAINING ONLY
OTHERWISE UNCLASSIFIED

Intelligence Markings

**National Classification Management
Society**

Twentieth Annual Training Seminar

Las Vegas

22-25 May 1984

Presented by:

**Ron Waavar
Office of Naval Intelligence
Chief of Naval Operations
Security Policy Division**

and

**David Whitman
Office of the Deputy Under Secretary of Defense (Policy)
Security Plans and Programs Directorate**

Introduction

This presentation addresses basic requirements for the use of intelligence markings.

The markings are authorized for use by the Director Central Intelligence to identify and control intelligence information. DCID 1/7 applies.

Definitions

Intelligence information and related materials includes the following classified information:

Foreign Intelligence-Information relating to the capabilities, intentions and activities of foreign powers, Organizations or persons.

Counterintelligence-Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

Information describing U.S. Foreign intelligence and Counterintelligence Activities, Sources, Methods, Equipment, or Methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained for exploitation; and photography or recordings resulting from U.S. Intelligence collection efforts.

Information on Intelligence Community protective security programs (a.g., personnel, physical, technical, and information security).

Warning Notice-Intelligence Sources or Methods Involved (WNINTEL/WN)

This marking is used to identify classified intelligence information whose SENSITIVITY REQUIRES CONSTRAINTS ON ITS FURTHER DISSEMINATION AND USE. This marking may be used only on intelligence which IDENTIFIES OR WOULD REASONABLY PERMIT IDENTIFICATION of an INTELLIGENCE SOURCE OR METHOD WHICH IS SUSCEPTIBLE TO COUNTERMEASURES THAT COULD NULLIFY OR REDUCE ITS EFFECTIVENESS.

Information so marked shall NOT BE DISSEMINATED IN ANY MANNER OUTSIDE AUTHORIZED CHANNELS WITHOUT THE PERMISSION OF THE ORIGINATING AGENCY AND AN ASSESSMENT BY THE SOTC IN THE DISSEMINATING AGENCY AS TO THE POTENTIAL RISKS TO NATIONAL SECURITY AND TO THE INTELLIGENCE SOURCES OR METHODS INVOLVED. In making such assessment, consideration should be given to reducing the risk to the intelligence sources or methods which provided the intelligence by sanitizing or paraphrasing the information so as to permit its wider dissemination.

Dissemination and Extraction of Information Controlled By Originator (ORCON/OC)

This marking is used to **ENABLE CONTINUING KNOWLEDGE AND SUPERVISION BY THE ORIGINATOR**. This marking may be used only on classified intelligence information which **CLEARLY IDENTIFIES OR WOULD REASONABLY PERMIT READY IDENTIFICATION OF AN INTELLIGENCE SOURCE OR METHOD** which is **PARTICULARLY SUSCEPTIBLE** to countermeasures that would nullify or measurably reduce its effectiveness.

Information bearing this marking **MAY NOT BE DISSEMINATED IN WHOLE OR IN PART** through briefings, incorporation into reports, or in any other manner outside the headquarters element of the recipient organizations, or used in taking investigative action, without the advanced permission of, and under conditions specified by, the originator.

NOTE: THIS IS THE MOST RESTRICTIVE MARKING, procedures will be established to ensure that this marking is applied to **PARTICULARLY SENSITIVE INTELLIGENCE** information and that timely procedures are established to review requests for further dissemination of intelligence information bearing this marking.

Not Releasable to Contractors/ Consultants (No Contract/NC)

This marking is used to identify classified intelligence information that **SHALL NOT BE RELEASED** to **CONTRACTORS** or **CONSULTANTS** without the permission of the originating agency. This marking may be used only on intelligence information which, if disclosed to a contractor, **WOULD** or **POTENTIALLY** give him a **COMPETITIVE ADVANTAGE** which could reasonably be expected to cause a **CONFLICT** of **INTEREST** with his **OBLIGATION** to **PROTECT** the information; or which was provided by a **SOURCE** on the **EXPRESS** or **IMPLIED** condition that it would **NOT BE MADE AVAILABLE** to **CONTRACTORS**.

NOTE: These restrictions do not apply to consultants hired under Office of Personnel Management procedures, or comparable procedures derived from statutory authorities of department or agency heads, and who are considered to serve as extensions of their employing offices.

Caution-Proprietary Information Involved (PROPIN/PR)

This marking is used with or without a security classification to identify information provided by a **COMMERCIAL FIRM** or **PRIVATE SOURCE** under an **EXPRESS** or **IMPLIED** understanding that the information will be protected as a **TRADE SECRET** or **PROPRIETARY DATA BELIEVED** to have **ACTUAL** or **POTENTIAL VALUE**.

Information bearing this marking **SHALL NOT BE DISSEMINATED** in any form to an **INDIVIDUAL, ORGANIZATION, or FOREIGN GOVERNMENT** which has any interests, actual or potential, in competition with the source of the information without the permission of the originator. This marking may be used in conjunction with the **NOCONTRACT** marking to preclude dissemination to any contractor.

Authorized for Release to (name of country(ies)/ International Organization) (REL)

This marking is used to identify classified intelligence that an **ORIGINATOR HAS PREDETERMINED TO BE RELEASABLE OR HAS RELEASED, THROUGH ESTABLISHED FOREIGN DISCLOSURE PROCEDURES and CHANNELS, to the FOREIGN COUNTRY(IES)/ INTERNATIONAL ORGANIZATION** indicated. No other foreign dissemination of the materiel is authorized (in any form) without the permission of the originator.

Not Releasable to Foreign Nationals (NOFORN/NF)

This marking is used to identify classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non U.S. citizens without permission of the originator. This marking may be used on **INTELLIGENCE WHICH IF RELEASED TO A FOREIGN GOVERNMENT OR NATIONAL(S) COULD JEOPARDIZE INTELLIGENCE SOURCES OF METHODS, OR WHEN IT WOULD NOT BE IN THE BEST INTERESTS OF THE UNITED STATES TO RELEASE THE INFORMATION FROM A POLICY STANDPOINT** upon specific determination by a **SOIC**.

SOICs are responsible for developing, publishing, and maintaining guidelines consistent with the policy guidance herein for use in determining the foreign releasability of intelligence they collect or produce. These guidelines shall be used in assigning **NOFORN** control markings, and by primary referents in responding to inquiries from other organizations on application of this control.

WORKSHOP 7

Classification Markings

SET # 1

CLASSIFICATION PENDING MARKINGA. WHEN AND HOW SHOULD THIS MARKING BE USED?

1. Only when the originator of the material does not have an applicable classification guide, DD Form 254, or has not extracted classified information from another document, but does believe the material should be protected based on previous experience in a similar field of interest which the government has acquired a proprietary interest. In this case the following marking should be applied to the document:

Classification determination pending
Protect as though classified
(INSERT CONFIDENTIAL, SECRET OR TOP SECRET)

2. The above marking need only to be applied once on the material but placed conspicuously so as to draw attention of the recipient. No other markings are required. However, if desired by the contractor, it is acceptable to add the designation "company private or "proprietary".

B. NOW WHAT STEP SHOULD BE TAKEN?

1. Send the document to an appropriate User Agency for a classification determination. Explain why the decision was reached that it perhaps should be classified. ("An appropriate User Agency" could be one of the following):

(a) The DoD activity wherein a current contractual relationship exists in a "like: atmosphere.

(b) The Head of a Military Organization.

(c) One of the Agencies listed on pages 250/251 of the Industrial Security Manual (ISM).

2. Limit the distribution of this information pending the results of the final classification determination and, of course, safeguard it accordingly.

C. If a response has not been received within thirty (30) days of submission to the appropriate User Agency, assistance may be requested from the contractor's Cognizant Security Office.

SET # 2

ADDITIONAL MARKINGS/SPECIAL ACCESS MARKINGS

In some instances, additional markings need to be assigned to classified documents or other material in addition to the overall classification of the document and appropriate "Classified by" and "Declassify on" markings as shown below:

A. RESTRICTED DATA/FORMERLY RESTRICTED DATA.

1. Restricted Data and Formerly Restricted Data markings are evidence of exemption from further downgrading/declassification instruction. However, "Classified by" is to appear on material generated after 1 June 1972 that is based derivatively on RD/FRD information.

2. Remarkings of RD/RFD material originated prior to 1 June 1972 is not required.

3. The following markings would be replaced in a conspicuous spot on the outside of the front cover, if any, or on the first page if there is no front cover in addition to the highest overall classification assignment applicable to the document.

Classified by: _____

RESTRICTED DATA

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

Classified by: _____

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act, 1954.

B. WNINTEL.

WARNING NOTICES

INTELLIGENCE SOURCES OR METHODS INVOLVED

1. This marking denotes material which contains classified intelligence information.

2. This marking is to be used when:

- (a) So directed by a classification guide or DD Form 254.
- (b) Extracting information from another document carrying this marking.

3. This marking is to be applied to the front cover, if any, or first page or title page of the document.

C. FOREIGN GOVERNMENT INFORMATION (FGI)

This marking is applied and used on the face of the document and used on documents which contain foreign government information to ensure that such information is not declassified prematurely or disclosed to a third country without consent of the originator.

D. NATO MARKINGS

There are two types of markings which relate to NATO INFORMATION:

- 1. The following marking is to be used on U.S. documents which contain extracts from NATO marked documents:

THIS DOCUMENT CONTAINS NATO INFORMATION

This notation is required to ensure that NATO information is not declassified or made accessible to nationals of non-NATO countries without NATO approval.

- 2. One of the following is to be used on documents to signify that the document is the property of NATO:

NATO SECRET
NATO CONFIDENTIAL
NATO RESTRICTED
COSMIC TOP SECRET

- 3. One of the above markings, as appropriate, would be applied to the outside covers, if any, or first page of the document.

E. CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI) MARKINGS

This marking is applicable when TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA reveals the theory of operation or design of the components of the thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device.

- 1. This marking would be applied when:
 - (a) So directed by a classification guide of DD Form 254.
 - (b) Information is extracted from another document carrying this marking.

2. The following represents the manner in which it is to appear on the front cover, if any, or first page or title page of the document:

CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION
DoD DIRECTIVE 5210.2 APPLIES

SET # 3

CLASSIFYING AUTHORITY AND DOWNGRADING DECLASSIFICATION INSTRUCTIONS

A. All information classified by an authorized official within the DoD must show the following:

1. Classified by: (See Below)

(a) Use the Date of the DD Form 254, plus Contract No. or IFP, RFQ, RFP No. as appropriate or the designated applicable User Agency Classification Guide.

(b) If "Multiple Sources" are also utilized - add And Multiple Sources" to 1(a) above. When using this additional statement - records must be maintained to support this phrase and retained for the duration of the contract or program for which the document was created.

2. Declassify on: (See Below)

(a) Show the date/event as designated by the DD Form 254 or User Agency Classification Guide.

(b) Most restricted source document date.

(c) Originating Agency's Determination Required (OADR) if:

(1) The DD Form 254 so designates.

(2) If the DD Form 254 or source material shows an indefinite date or event, declassification review date, or no date or event for declassification.

B. The following is not required marking and is used only as stated below:

Downgrade to _____ on _____ (See Below)

1. Use if directed to do so by the DD Form 254 or User Agency Classification Guide or as shown on a source document.

2. Insert SECRET or CONFIDENTIAL and indicate the effective date or event as designated.

C. The following samples of the above are provided:

Classified by: DD Form 254, 28 February 1982, Contract
N00123-82-C-1234.

Declassify on: 31 December 1988

Classified by: OPNAVINST 1234.5, 1 March 1980

Declassify on: Originating Agency's Determination Required

Classified by: DD Form 254, 3 April 1981, Contract
N00030-81-R-5678 and Multiple Sources
Downgrade to CONFIDENTIAL on 5 May 1988.

Declassify on: 31 December 1990.

SET # 4

REMARKING CLASSIFIED MATERIAL ORIGINATED PRIOR TO AUGUST 1982

Material originated prior to 1 August 1982 which specifies a date or event for declassification need not be remarked unless:

1. Such direction has been received from the originator, User Agency or by a Revised/Final Form 254.

2. If the document is withdrawn for use, such as for the purpose of extracting from it, reproduction purposes, or if the document is transmitted outside the Agency or Facility.

MARKING OF COMPILATIONS

In some instances, certain information would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, portions of a document classified in this manner need not be portion marked.

MARKING OF WORKING PAPERS

1. Working papers include such things as NOTES, DRAFTS, DRAWINGS, AND OTHER WORK IN PROCESS material accumulated or created in preparation of a finished document. This material is to be:

(a) Marked with the overall classification and appropriate page markings.

(b) Dated when created.

2. Working papers do not require portion marking and downgrading/declassification instructions until such time as the material is entered into the accountability system, made a part of a permanent records or dispatched outside the facility/activity.

SET # 5

CLASSIFICATION MARKINGS/SYMBOLS

A. FRONT COVER, TITLE PAGE, OR FIRST PAGE MARKING -

1. A properly marked Front Cover, Title Page and First Page will show the overall classification at the top and bottom, the document title with the appropriate classification symbol in parenthesis after the title, date of the document, the appropriate classification authority, etc., and the full address of the facility or agency.

B. PAGE MARKING -

1. Interior pages will be marked at the top and bottom of each page with highest classification contained on that page, or designation of UNCLASSIFIED if all portions on the page are UNCLASSIFIED.

(a) As an alternate, overall document classification may be marked at the top and bottom of each interior page when necessary to achieve production efficiency.

(b) Classification of the information must be adequately identified in accordance with portion marking requirements.

C. COMPONENT MARKING -

In cases wherein there are major components to complex documents, each major component can be marked as a separate document utilizing all other classification marking requirements.

D. PORTION MARKING - (Section, Part, Paragraph or Similar Portion)

1. Mark each portion to eliminate doubt about the level of classification.

2. Mark each portion with its highest classification or mark it UNCLASSIFIED.

3. Mark each portion immediately following its number or letter designation.

OR

Before it begins if there is no number or letter designation.

E. PORTION MARKING - FOREIGN GOVERNMENT, NATO INFORMATION, OR CNWDI INFORMATION -

1. When foreign government information is included in U.S. documents, that information must be marked to reflect the originating

country as well as the level of classification, i.e., CANADA-R, U.K.-S, NATO-S.

2. The above markings would not be applied when the fact that foreign origin must be concealed.

3. Portions of a document containing "Critical Nuclear Weapons Design Information" shall be marked with an (N) following the classification assigned to that portion, i.e., (S-RD) (N).

F. MARKING MATERIAL OTHER THAN PAPER COPIES OF DOCUMENTS -

The following procedures for marking various material containing classified information are not all inclusive.

1. Conspicuously stamp, print, write, paint, or affix the classification assignment and other applicable associated markings to the material so that all holders will be aware of the protection required.

G. MARKING CHARTS, MAPS, DRAWINGS, AND TRACINGS -

1. Mark the legend, Title or scale blocks, in a manner that differentiates between the classification of the document and the legend or title.

2. Mark overall classification on the top and the bottom of the document.

3. When folded or rolled, classification markings must be visible.

4. Applicable associated markings shall be included near the legend or title block.

H. MARKING PHOTOGRAPHS, FILMS, AND RECORDINGS -

1. Mark to ensure that the recipient, viewer, or listener will know the classification.

I. MARKING MAGNETIC, ELECTRONIC OR SOUND RECORDINGS -

1. A clear statement of the classification at the beginning and the end is required.

2. Containers are to be marked with the appropriate classification and other applicable markings.

J. MARKING FILMS AND VIDEOTAPES

1. Mark the beginning and end of each reel with the classification and applicable markings so that these markings are visible when projected.

2. Mark the containers with appropriate classification and applicable associated markings.

K. MARKING PHOTOGRAPHS -

1. Negatives and positives must be marked with the appropriate classification and applicable associated markings.

2. Roll negatives or positives may be so marked at the beginning and end of each strip.

3. Containers for negative and positives shall be conspicuously marked with the highest level of classification of their contents as well as any other additional (special) marking.

4. All prints and reproductions shall be conspicuously marked with appropriate markings above the face side of the print, if possible. When not possible to do so, they may be stamped or marked on the reverse side or affixed by pressure tape level, stapled strip, or other comparable means.

L. MARKING TRANSPARENCIES, VUGRAPHS, AND SLIDES

1. Classification assignment must be shown in the image area whenever possible. When not possible to do so, mark the border, holder, or frame. Other applicable markings shall be shown on the border, holder, or frame when it is not possible to show them in the image area or in the accompanying documentation or other written notification.

2. When a set of such material is controlled as a single document, only the title slide or transparency requires the other applicable markings. However, if individual slides or transparencies are removed from the set, they must be marked with all appropriate markings.

M. MARKING MICROFORMS (Microfiche, Microfilm, Micor Atrips and Chips, Aperture Cards)

1. The classification assignment and abbreviated applicable associated markings on the medium or container must be readable with the unaided eye.

2. The classification markings within the image area must be readable when displayed.

3. The classification markings must appear at the beginning and end of each roll of microfilm.

4. Decks of aperture cards must be marked with the classification on the first and last cards.

5. Decks of aperture cards must contain a card identifying contents of the deck, the highest classification, and applicable associated markings.

N. MARKING REMOVABLE ADP AND WORD PROCESSING STORAGE MEDIA

1. Removable information storage devices must bear external markings indicating classification and applicable associated markings.

(a) Examples of removable storage devices include:

Magnetic Tape Reels	Diskettes
Cartridge & Cassettes	Paper Tapes
Disk Cartridges	Removable Disks
Disk Packs	Magnetic Cards

2. ADP Systems and word processing systems employing such media shall provide for internally recorded security classification markings to assure that classified information contained therein, which is produced or generated will bear applicable classification and associated markings.

O. MARKINGS DOCUMENTS PRODUCED ON ADP EQUIPMENT

1. Conspicuously mark or stamp classification on the first page, and front and back covers, if any.

2. Apply other applicable markings on the face of the document.

3. The classification on the interior pages may be applied by the equipment.

4. If individual pages are removed or reproduced, they must be marked as a separate document.

P. MARKING DECKS OF ADP PUNCHED CARDS

1. When controlled as a single document, only the first and last cards require classification markings.

2. The deck must contain a card identifying contents, highest classification and applicable associated markings.

3. Cards removed and not returned immediately to the deck must bear appropriate classification markings.

(a) A group of cards so removed may be controlled as a separate document and so marked.

Q. MARKING FILE FOLDERS

1. Files, Folders, Binders, Envelopes, etc., containing classified documents when not in secure storage shall be conspicuously marked according to the highest classification of any classified document included therein.

2. Classified document cover sheets may be used for this purpose.

(for training purposes only)

LAST PAGE

(for classified document
marking practical exercise)

1. This page contains no classified information. Please put the correct classification at the top and the bottom of the page.

NOTE: The following are problems and have nothing to do with portion marking on this page or the classification of the page.

A. () This portion contains SECRET RESTRICTED DATA. Please fill in the bow-legs.

B. How would you mark, or change the marks, on the front and back covers of this document if it contained SECRET RESTRICTED DATA? _____

Would you change the markings on pages of this document (other than the portions) if it contained SECRET RESTRICTED DATA? _____

C. () This portion contains CONFIDENTIAL FORMERLY RESTRICTED DATA. Please fill in the bow-legs.

D. How would you mark, or change the marks, on the front and back covers of this document if it contained CONFIDENTIAL FORMERLY RESTRICTED DATA? _____

Would you change the markings on pages of this document (other than the portions) if it contained CONFIDENTIAL FORMERLY RESTRICTED DATA? _____

E. () This portion contains CNWDI classified SECRET. Please fill in the bow-legs.

F. How would you mark, or change the marks, on the front and back covers of this document if it contained CNWDI classified SECRET? _____

Would you change the markings on pages of this document (other than the portions) if it contained CNWDI classified SECRET? _____

G. () This portion contains NATO SECRET information. Please fill in the bow-legs.

H. How would you mark the cover(s) if the document contains NATO SECRET information? _____

NOTE: This is the last page of your study document.

(for training purposes only)

PART III
Annual Report
and
Awards

20th ANNUAL REPORT

1. The general business meeting of the Twentieth Board was called to order by President John Puckett at 9:05 AM. President Puckett thanked Mike Lower and his committee for their hard work and excellent organization. He also thanked the attendees and encouraged them to take their training and new ideas back to their facilities.
2. President Puckett stressed that his goals as mentioned at the Fort Worth seminar last year were:
 - a. Continue membership growth. This has been outstanding (see Membership report).
 - b. Four new chapters. Three were formed this year:
 - (1) Texas Gulf Coast;
 - (2) Mid-South;
 - (3) Florida Sun Coast;
 - c. Continue training & education
 - (1) A mini-seminar was held at Albuquerque, New Mexico with 100 plus attendees. Betty Boutwell and Dick Fredlund were to be commended.
 - (2) Training materials have been placed in the Bulletins. Gene Suto has instituted this program.
 - (3) The Education Committee chaired by Jim Mathena has made available training literature from the Executive Secretary.
 - d. Finally the Bulletins and Journal are back on track. In this connection the latest Journal should be at your office when you return home. Gene and Barbara Suto were commended for their fine work for the society.

3. The 20th Board of Directors was listed as follows:

President	John E. Puckett
Vice President	Pamela M. Hart
Secretary	Elaine R. Gruber
Treasurer	Irving T. Boker
Director	Gerald L. Berkin
Director	Clarissa M. DeAngelis
Director	Robert R. Fredlund, Jr.
Director	Elizabeth M. Heinbuch
Director	Bill Johnson
Director	James A. Maneggie
Director	James H. Mathena
Director	Robert C. Moore
Director	Sandra Waller
Executive Secretary	Eugene J. Suto
Deputy Executive Secretary	Barbara H. Suto
Counselor Emeritus	Donald B. Woodbridge

4. Mr. Puckett stated the following about the Society at Work
 - a. Annual Seminars are held which are the heart and soul of the society. He stated the benefits of the Seminars—both national and minis are many—but the most important are:
 - (1) Affords an opportunity to hear the latest policy changes and future trends that affect our profession. You get this information from the individuals and Agencies who are responsible.
 - (2) If you are a novice in the profession—the seminars give you hands-on training opportunities at the "nuts and bolts" level. For example, workshops on basic security contract administration, How to read or prepare a Form DD 254—recognizing things could cause a major impact on the contract in terms of cost, manning, etc. Perhaps even more importantly, you learn who you can go to for help. This can pay big dividends in the areas of gain-

ing professional respect from your own peers and management, not to mention the savings in time and money.

- (3) This leads to another important society benefit—That of personal contacts—not only do you meet and hear your counterparts in Government and Industry in formal presentations, there is also ample time to talk and discuss mutual problems on a one-on-one. You will be amazed at the red tape you can cut and how much you can increase your efficiency if you are able to pick up telephone and talk to a counterpart that you have met or know through the Society.
5. The Publications of the Society are another set of tools that you will find invaluable in your work. These are:
 - a. The Bulletin. This publication is designed to keep you current on information security and classification management events in our profession. It contains training aids such as sample briefings and various "how to" advice. It will also keep you informed as to what the Society as a whole is up to.
 - b. The Journal. Normally published annually is the proceedings of the annual seminar. It is a valuable reference and training device.
 - c. The Directory. Published twice each year provides you with names, addresses and phone numbers of fellow members—This puts an awful lot of help and advice at your fingertips.
6. The *Membership Report* by Pamela Hart is as follows:

Total number of members: 860
Total number of members on 6/21/83: 711
Net increase in members of 149 in eleven months
7. The *Treasurer's Report* by Irving Boker indicated the total assets on hand as of January 1, 1984, was \$46,800. Total assets on hand as of May 22, 1984, is \$56,400.
8. The *Finance Committee Report* by Gerald Berkin indicated the financial records are in excellent condition. There was a net loss for 1983 of \$2,958. Total assets as of December 31, 1983, are \$46,950. The Society's financial condition is sound.
9. The *Nomination Committee Report* by Sandra Waller disclosed that a total of 906 ballots were mailed. 504 ballots were returned, 55.6%. The following members have been elected to three-year terms on the Board of Directors:

Gerald L. Berkin
Betty E. Boutwell
Pamela M. Hart
Carol A. Thomas
10. President Puckett presented awards to persons responsible for formation of three new chapters:
 - a. Texas Gulf Coast Chapter awards were to:

E. Neil Self
Michael E. Corbin
Selena M. Post
 - b. Mid-South Chapter awards were to:

Bill Johnson
Charley A. McMinn
Terris C. Lewis
 - c. Florida Sun Coast Chapter awards were to:

Ellen S. Herndon
Rick H. Batchelor
Louisa M. Blackwell
11. Plaques were presented to out-going Board members Elaine Gruber and Elizabeth Heimbuch, and to two Board members who were re-elected for second terms Gerald Berkin and Pamela Hart.
12. President Puckett read the citation and presented to Eugene J. Suto the Donald B. Woodbridge Award for Excellence as follows:

DONALD B. WOODBRIDGE
AWARD OF EXCELLENCE
CITATION

During the period from 1964 through 1983, Eugene J. Suto promoted, devised, and wrote many of the major directives for the Department of the Army implementing the program for the identification and protection of information affecting the national security. He actively participated in the development and application of sound classification management throughout the Department. During the early 1970s, Mr. Suto initiated and was responsible for leading a major program directed at the review of the Department of the Army's intelligence records for World War II. For this program he recruited and led many Army Reserve Intelligence Officers conducting the review and was responsible for drafting and revising guidelines used in the declassification review and determination process.

Mr. Suto regularly contributed to the development of the several Executive Orders prescribing the information security program since Executive Order 10501. He actively participated in ongoing efforts to develop national implementing directives for two Executive Orders and meaningfully contributed to the Department of Defense's implementing regulation for those orders.

Mr. Suto provided information to and appeared before the several interested Congressional Committees conducting both oversight hearings and considering legislation in the field of information security. He participated in the development of the National Classification Management Society's position on the question of a legal foundation for the security classification of information. While serving as the President of the Society he presented the position paper to the requesting Congressional Committee.

Mr. Suto has been notably active in the area of education in classification management. Through his personal efforts both in the Society and in other organizations, he has extended the horizons of many individuals nationwide in the purposes of and need for sound classification management.

Mr. Suto has contributed his personal effort extensively in the development of the National

Classification Management Society. Twice he served as its president, he served twelve years as a Director, he held many other national as well as chapter offices, he was chairman or member of innumerable committees, and regularly contributed to the production of and authored several important articles in the Society's publications. His unfailing dedication to the purposes of the Society also merit recognition.

Eugene J. Suto has served his country well through his perseverance and dedication to well-considered and positive classification management policies and programs. By his long-time personal efforts and numerous valuable contributions he exemplifies the high standards suitable for recognition by the National Classification Management Society in presenting him with the *Donald B. Woodbridge Award of Excellence* in Classification Management.

13. President Puckett introduced the officers and directors of the Twenty-first Board of Directors as follows:

P. Hart—President-elect
I. T. Boker—Vice President-Elect
S. J. Waller—Secretary-elect
R. Moore—Treasurer-elect
G. L. Berkin—Director
B. E. Boutwell—Director
C. M. De Angelis—Director
R. R. Fredlund—Director
Bill Johnson—Director
J. A. Maneggie—Director
J. H. Mathena—Director
J. E. Puckett—Director
C. A. Thomas—Director

14. The annual business meeting was closed at 9:45 A.M.

PART IV
20th Seminar
Charter Members Program
and
Seminar Photos

PART FOUR

20th Seminar Charter Members Program

Charter Member Program, Fred Daigle	195
Letters from Past Charter Members	198
Picture of Founders	199
Charter Members	200
First National Seminar	204
Past Presidents	204
20th Anniversary Opening Ceremonies	205
Awards to Chapter Chairmen, Directors and Woodbridge Award	206
20th Anniversary Reception	207
Charter Member Awards	210
Seminar Speakers	212
Workshop Speakers	214
Seminar Committee	214
Current Board Members	215

THE BIRTH OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

**Frederick J. Daigle, Lockheed
Missiles & Space Company Inc.
Sunnyvale, California**

In his inaugural speech in 1973 then president Nixon made an observation that in some form or another must have been in the minds and hearts of the founders of NCMS. He said "abroad and at home, the time has come to turn away from the condescending policies of paternalism—of Washington knows best. That is why I offer no promise of a purely governmental solution for every problem. We have lived too long with that false promise. In trusting too much to government, we have asked of it more than it can deliver. This leads only to inflated expectations, to reduced individual error and to a disappointment and frustration that erode confidence both in what government can do and what people can do."

Eleven years later, the same philosophy prevails, we must continue to turn away from the policies of paternalism of Washington knows best.

The credit for the initial efforts toward the founding of the National Classification Management Society rests with a small group of individuals who were then part of the only recognized group involved in this new world of classification,

namely, the classification personnel of the Atomic Energy Commission (AEC) family.

Early in the spring of 1963, a need for improving communications between the classification people of the nuclear design laboratories and those of the nuclear production agencies was recognized. It was at this time that the idea was conceived of establishing a professional society in the field of security classification management for AEC government and contractor personnel. Discussions were held that spring by Richard Durham, Classification Officer, Sandia Corp., Livermore Laboratory, Calif., with James Ruff, then Classification Officer at Lawrence Radiation Laboratory, Livermore, Ca., and with Doctor Leslie M. Redman of the Los Alamos Scientific Laboratory, New Mexico. The three of them agreed that this would be an appropriate item for discussion at the first meeting of the Weapon Contractors Classification Conference (WCCC) working group which was to be held June 4 and 5, 1963, at the Bendix Corporation's Kansas City Division.

In attendance at that first meeting of the WCCC were: James Marsh, Classification Officer and Charles Prohasdka, Classification Analyst, Sandia Corporation, Albuquerque; Les Redman, Donald Woodbridge and Robert Dreyer, Classification Officers, Union Carbide Nuclear Company, Oak Ridge, Tenn.; Edward Caivert, Classification Officer, South Albuquerque Works AFT Industries Inc.; Dick Durham, Classification Officer Sandia Corporation, Livermore Laboratories, Calif.; James Bunch, Classification Officer, Pantex Company, Amarillo, Texas; and the host, Jack Long, Classification Officer, Bendix Corporation, Kansas City Division.

On June 5th, the second day of the meeting, the idea of forming this professional classification management society was discussed in depth and all attendees agreed that it was worthy of further investigation and effort.

Discussion ensued as to the advisability of associating our organization with the American Society for Industrial Security (ASIS). It was further agreed to talk to DoD contractor personnel and a meeting was scheduled for November 20, 1963.

In the interim, DoD contractors were contacted

and so was an ASIS chapter officer who agreed to raise the question with the ASIS directors. Five months later, no response was received from ASIS.

The contacts with DoD contractor personnel was most fruitful, however, and on the afternoon of November 20, 1963, in the conference room of Sandia Corporation, Livermore, twenty three classification representatives from DoD contractors, AEC contractors and field classification personnel of the AEC met, considered the idea favorably and organized a steering committee. The ad hoc steering committee consisted of John Shunny, Sandia Corporation, Albuquerque; Robert Rushing, Lockheed Missiles and Space Company, Sunnyvale, Ca., William Herling, Space Technology Laboratory, Redondo Beach, and Richard Durham, Sandia Corporation, Livermore. John Shunny was named Chairman and Dick Durham Secretary/Treasurer of the committee.

The first duties of the committee were to solicit assistance from other interested persons in the then sparse classification community, draft bylaws, and select a name for the blossoming organization. During this meeting it was suggested and acted upon that those present, so inclined, contribute \$10 to help build a treasury to cover initial costs. This contribution would eventually become the members initiation fee which was also set at \$10 as was the annual dues.

As of December 18, 1963, the following were considered the very first chapter members of the society. From the AEC community: Ed Calvert; Dick Durham; James Patterson, then of Sandia Livermore Laboratory; and, John Shunny. From the defense industry group: Fred Daigle; Lyle Dunwoody; Bob Rushing; and, John Wise all of Lockheed Missiles & Space Company in Sunnyvale, California.

By December 18, 1963, the steering committee had agreed, after considerable research and study, on the official title of "National Classification Management Society," and the draft bylaws were published and disseminated to the charter members and the prospective charter members. It is worthy to note here that the society has seen no need to change the name of the society, even though we are now information security oriented, an expansion of our original Classification Management (CM) concept.

The main driving forces during the initial founding phase, prior to the incorporation of the society were, without any question of doubt, Bob Rushing and John Shunny.

By January 16, 1964, the formal charter members had grown by the addition of Jim Marsh, and Lorry McConnell of Systems Development Corporation, Santa Monica. Major A. A. Correia, then of Norton AFB, Ca., became our first military member, and Francis W. May then of Air Force Headquarters was our first government civilian employee to become a member.

On March 31, 1964, the society was incorporated as a nonprofit professional society; under the laws of the state of New Mexico, and, as such, the society formally and legally came into being.

As of 13 May 1964, the society had grown to 35 charter members, and the treasury held \$495.00. On 11 August a letter was sent to all charter members furnishing a slate of officers for the initial NCMS directorships.

On 17 September the ballots had been counted and the board of directors were selected as follows: Dick Durham, Bob Rushing, Don Woodbridge, Tony Correia, Les Redman, Bill Herling and Bob Niles.

From among the board, officers were elected as they are today, naming Don Woodbridge as Chairman of the Board (a position later eliminated), Bob Rushing, President, Dick Durham, Vice President, and Bill Herling, Secretary Treasurer (a task later divided into two positions). Plans were immediately underway to hold the first seminar in 1965. Washington, D.C., was selected as the site and Dick Durham was given the job of Seminar Chairman and Gene Suto the Secretary/Treasurer.

During this same period, other activities were taking place all over the country in the form of organizing area chapters.

Under the leadership of Dick Durham, the first organization meeting of the Washington, D.C., chapter and perennially our largest chapter was held in November 1964 with forty interested persons attending. Mr. Don Garrett, then of the Office of the Secretary of Defense was selected as first

Chapter Chairman and Gene Suto, Secretary/Treasurer. Almost concurrently, in northern California, under the guidance of Fred Daigle, the first organizational meeting of the then Bay Area Chapter was held in October 1964 and the chapter formally organized in December 1964. Fred was elected the first chapter chairman, a position he held for the first two years of the chapters organization. This chapter was renamed the Northern California Chapter and although small in number for many years, proved to be very innovative and hosted the fourth national seminar in 1968.

The Southern California cadre of members was not idle. Although even fewer in numbers (a situation they soon corrected under the leadership of Lorimer (Lorry) McConnell) they undertook the task of organizing a chapter in 1964 with the final organization meeting in 1965. Southern California, although it only started with three members, continually grew and provided a challenge to Washington as the largest chapter until it self divided and a portion of its membership created the San Diego Chapter. Southern California hosted the first seminar held outside the Washington area (in 1966), and have consistently pioneered in conducting successful seminars in and outside of Los Angeles at remote locations such as San Diego and of course here in Las Vegas. Believe me that is no easy task, they seem to make it look like it was.

In the spring of 1965 only 16 months after the first exploratory meeting at Livermore, the first issue of the Journal appeared under the editorship of Dr. Les Redman. This Journal announced the program for the first national seminar and contained articles by Robert Pushing, George MacClain, Director of Classification Management, Office of the Assistant Secretary of Defense, Dick Durham, Mr. C. C. Carnes, Jr. then of Dow Chemical and by Fred Daigle. Our bylaws and first membership list of 71 members was included.

Since then the Journal has undergone many changes not only in content but in appearance. The Journal has been registered as an information source by the National Referral Center, Science and Technology Division, Library of Congress.

The C. M. Intelligencer was our first Bulletin although many of you have never heard of this

document, it was the granddaddy of our current C. M. Bulletin. First issued as the Northern California Chapter Newsletter by Robert Donovan, then of United Technology, Sunnyvale, the Intelligencer gained national recognition and evolved into the early version of our CM Bulletin with the first edition published in November 1967. This early bulletin was authored by Bob Donovan and printed, assembled and mailed by Gene Suto, Research Analysis Corporation and his four girls with headquarters located on the floor of the Suto living room about twenty feet from the current location of the NCMS executive office.

Our bulletin has travelled a long road to its present format, content and editorial policy. It had many editors including Don Garrett, Frank May, Gene Suto, James Marsh, Fred Daigle, Don Woodbridge and Jim Bagley. However, we owe its continued existence and its current format to Jim Buckland and Jack Robinson who provided its survival until finally returning the responsibility for editing and publication to our Executive Secretary, Gene Suto.

Our seminars are the life blood of the society. They are the only training seminars in the United States dedicated to the DoD information security program. They are attended by all echelons of information security practitioners. Look around you, we are over 400 strong this year, the largest ever, and look at the pictures in the lobby of the first seminar. We've come a long way but only through your loyalty and effort. Enjoy the next four days, meet everyone here, lunch with different table mates every day, not with your boss, your fellow workers or your friends, this is the place and the time to make those new contacts. I'm sure you will join with me and say thank you founders of NCMS and thank you charter members. Your tenacity in 1963 and 1964 is paying off in 1984, and we hope those founders and charter members who were not able to join us today can fully realize how much we mean by "thank you." We will meet those founders and charter members who were able to join us here in Las Vegas during a special program to be held during the President's Reception, which our President John Puckett has very thoughtfully dedicated to us, the founders and charter members.

LETTERS FROM PAST CHARTER MEMBERS

Following are some extracts of letters from a few charter members who were unable to attend the Seminar:

Dear Fred:

Twenty years sounds like an awful long time but it doesn't seem that long ago that we started NCMS. Who would have thought that it would take hold the way it has. Certainly, the people who have been the kingpins in keeping it going have to be given full credit for maintaining and improving the value and activities of the organization. Much thanks and huzzahs for them!!!

Sure wish I could make it to the seminar and the CM reception, but can't do it. Don't hear from many of the old gang but do keep in touch with Dick Durham, Frank May, George MacClain. Guess you know Dick retired on 30 March. George has finally closed his law office and is really retired, trying to beat his wife at golf. Frank seems to keep busy playing golf between here and Florida the last I heard. Me? My wife keeps me travelling around hither and yon for bridge tournaments.

Give my regards to all the gang—have fun and stay happy!!

Best wishes to all. Thanks for thinking of me and the CMers.

DON GARRETT

EDITOR'S NOTE:

Don was a charter member, first chairman of the Washington Chapter, Member of the Board of Directors 1966-1969, and National Vice President—1967.

Dear Fred:

The enclosed might be of some interest to you at this particular time. It was my list of the original NCMS membership, arranged according to when the membership fee was paid. (I

was acting Secretary-Treasurer, pending election of officers.)

I guess I arbitrarily ranked people (Durham No. 1, Rushing No. 2, etc.) on the basis of some information I had at the time. It probably would have been better to have ranked all the 11/63 people as tied for No. 1. I see that of the first nine members, four were from Lockheed.

Good luck with the big meeting. I hope it turns out well. I may make it. My wife has never seen "Lost Wages" and would like to. But we have potential conflicts. In view of my uncertainty, please do not plan for my presence—in connection with the gifts, etc. Thank you very much for the call and the invitation.

Best Regards,
ED CALVERT

EDITOR'S NOTE:

Ed was one of the founding fathers who attended the first organization meeting in June 1963. He was also Journal editor from 1966-1970.

Dear Fred:

Thanks for your friendly note. I'm delighted to learn that the Society is doing so well and that the seminars continue. Although retired for nearly five years from Los Alamos Scientific Labs, I'm still working as a manager in classifications both in the review of vintage documents and on a project to put DoE classification guidance into a database. Bob Dreyer and Don Woodbridge joined in for the earlier project on review of old documents in 81-82 at Oak Ridge.

My Regards to Everyone,
LES REDMAN

EDITOR'S NOTE:

Les attended the first organization meeting of NCMS, was a member of the Board of Directors from 1964-1968, and was the first editor of the C.M. Journal.

PICTURE OF FOUNDERS



The first meeting of the Weapon Contractor Classification Working Group was held at Bendix-Kansas City on June 4-5, 1963. Individuals pictured above are, seated left to right, R. L. Durham, J. G. Marsh, J. E. Long, E. H. Calvert, James Bunch, standing left to right, R. C. Dreyer, C. R. Prohaska, L. M. Redman, D. B. Woodbridge

CHARTER MEMBERS**National Classification Management Society Membership**

CHARLES M. ATKINSON
 Defense Atomic Support Agency
 Washington, D.C.
 Phone: OXford 54318

****JAMES JOSEPH BAGLEY**
 U.S. Naval Research Laboratory
 Washington, D.C.
 Phone: 574-2576

ROBERT L. BECKNER
 TRW Space Technology Laboratories
 One Space Park
 Redondo Beach, California
 Phone: 679-8711, Ext. 11934

JACK M. BERKUS
 System Development Corporation
 2500 Colorado Avenue
 Santa Monica, California
 Phone: EX 39411

RICHARD J. BOBERG
 Aerospace Corporation
 2400 East El Segundo Boulevard
 El Segundo, California
 Phone: 648-7466

JOSEPH J. BOYLE
 United States Air Force
 Air Force Systems Command
 Air Force Missile Development Center
 Holloman AFB, New Mexico
 Phone: GR. 36511, Ext. 46153

JAMES E. BUNCH
 Mason & Hanger—Silas Mason Co.
 Amarillo, Texas

JOHN J. BURDETTE
 General Electric Company
 Light Military Electronics Dept.
 French Road
 Utica, New York
 Phone: SW. 71000, Ext. 5034

EDWARD H. CALVERT
 ACF Industries, Inc.
 P.O. Box 1666
 Albuquerque, New Mexico
 Phone: 247-0361

LEO D. CARL
 United States Air Force (AFISL-3C)
 Tempo "E", 6th & Adams, S.W.
 Washington, D.C.
 Phone: OXford 67941

CECIL C. CARNES
 502 Ord Drive
 Boulder, Colorado
 Phone: 443-8937

***MAJ. ANTONIO A. CORREIA**
 United States Air Force
 Ballistic Systems Division
 Norton Air Force Base, California
 Phone: TUrner 94411, Ext. 6058

JOHN E. COYNE
 North American Aviation, Inc.
 1700 East Imperial Highway
 El Segundo, California
 Phone: OR. 09151, Ext. 3737

***FREDERICK J. DAIGLE**
 Lockheed Missiles and Space Company
 111 Lockheed Way
 Sunnyvale, California
 Phone: RE 94321, Ext. 24139

****ROBERT C. DREYER**
 Union Carbide Nuclear Company
 Oak Ridge, Tennessee

STEVEN B. DUDLEY
 Lockheed Missiles and Space Company
 111 Lockheed Way
 Sunnyvale, California
 Phone: RE 94321, Ext. 24139

LYLE J. DUNWOODY, Jr.
 Lockheed Missiles and Space Company
 111 Lockheed Way
 Sunnyvale, California
 Phone: RE 94321, Ext. 21597

R. L. DURHAM
 11232 Waycross Way
 Kensington, Maryland
 Phone: 949-7577

JOHN EICHELBERGER
 Monsanto Research Corporation
 Mound Laboratory
 Miamisburg, Ohio
 Phone:

****DONALD C. GARRETT**
 Office Deputy Asst. Sec. Def.
 Pentagon
 Washington, D.C.
 Phone: OXford 75568, OXford 74917

ROBERTO R. GARZA
System Development Corporation
2500 Colorado Avenue
Santa Monica, California
Phone: EX 39411, Ext. 7214

ELWIN B. GODWIN
Autonetics
3370 Miraloma Avenue
Anaheim, California
Phone: 772-8111, Ext. 4505

CLINTON D. HAMILTON
United States Air Force
Hq. A.D.C. (ADCIG-3)
P.O. Box 16
Ent Air Force Base, Colorado
Phone:

ROBERT K. HEBBLEWHITE
Aerospace Corporation
1111 West Mill Street
San Bernardino, California
Phone: TUrner 49211, Ext. 1023

BOYD H. HEMPEN
McDonnell Aircraft Corporation
P.O. Box 516
St. Louis, Missouri
Phone: PE 12121, Ext. 2171, 2924

VIRGIL H. HERALD
General Precision Inc.
Librascope Group
808 Western Avenue
Glendale, California
Phone: 245-8711, Ext. 1415

WILLIAM J. HERLING
TRW Space Technology Laboratories
One Space Park
Redondo Beach, California
Phone: 679-8711, Ext. 11/33

JOSEF W. HEYD
Monsanto Research Corporation
Mound Laboratory
Miamisburg, Ohio
Phone:

JAMES A. HOWE
ARO, Inc.
Arnold Air Force Station, Tennessee
Phone: 455-2611, Ext. 382

HENRY B. INGARGIOLA
Stanford Research Institute
Menlo Park, California
Phone: 326-6200, Ext. 3168

JEAN C. INGHAM
Hughes Aircraft Company
Building 121-M/S1
P.O. Box 90515
Los Angeles, California
Phone: 670-1515, Ext. 6187

FRANCIS X. JAHN
Westinghouse Electric Corporation
P.O. Box 1693
Baltimore, Maryland
Phone: 761-1000, Ext. 3378

FRED A. KOETHER
Advanced Research Projects Agency
OSD, Pentagon
Washington, D.C.
Phone: 697-8904

JACK E. LONG
The Bendix Corporation
Kansas City, Missouri
Phone: EM 33211, Ext. 3325

HARRY C. LOUDENSLAGER
Battelle Memorial Institute
505 King Avenue
Columbus, Ohio
Phone: 299-3191 Ext. 422

WALTER A. LUCAS
System Development Corporation
P.O. Box 1326
Offutt Air Force Base, Nebraska
Phone: 393-8300

GEORGE MacCLAIN
Office of Asst Secy Def (Manpower)
Room 3 C 285
Pentagon
Washington, D.C.
Phone: OXford 75568, 73969, 74917

L. F. McCONNELL
System Development Corporation
2500 Colorado Avenue
Santa Monica, California
Phone: EX 39411

MILTON W. McFARLIN
Lockheed Missiles & Space Company
111 Lockheed Way
Sunnyvale, California
Phone: 739-4321

HOWARD G. MAINES
National Aeronautics & Space Admin.
Washington, D.C.
Phone: WO 21153

J. G. MARSH
Sandia Corporation
Sandia Base
Albuquerque, New Mexico
Phone: 264-3170

**FRANCIS W. MAY
United States Air Force Hqs.
(AFISL) Building T-E
4th & Adams Drive, SW
Washington, D.C.
Phone: CA 22314

PETER J. MOGLIA
Hughes Aircraft Company
Building 121 M/S1
P.O. Box 90515
Los Angeles, California
Phone: 670-1515, Ext. 6121

JAMES D. MORAN
General Precision, Inc.
Aerospace Group
Little Falls, New Jersey
Phone: 256-4000, Ext. 562

JOHN T. MURPHY
Space General Corporation
El Monte, California
Phone: 443-4271, Ext. 1172

IRL E. NEWLAN
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, California
Phone: 354-3360

**ROBERT G. NILES
Defense Atomic Support Agency
Pentagon
Washington, D.C.
Phone: OXford 54318

EDGAR G. OSBORN
Lockheed Missiles and Space Company
P.O. Box 504
Sunnyvale, California
Phone: RE 94321, Ext. 21597

JAMES H. PATTERSON
Sandia Corporation
Livermore Laboratory
P.O. Box 969
Livermore, California
Phone:

MARLYN R. POWELL
System Development Corporation
2500 Colorado Avenue
Santa Monica, California
Phone: EX 39411, Ext. 7322

JANE O. REDER
System Development Corporation
2500 Colorado Avenue
Santa Monica, California
Phone: EX 39411, Ext. 7675

LESLIE M. REDMAN
University of California, LASL
Los Alamos, New Mexico
Phone: 7-4196

ROBERT J. RUSHING
Lockheed Missiles and Space Company
111 Lockheed Way
Sunnyvale, California
Phone: 742-8316

*GEORGE E. SANDERS
System Development Corporation
2500 Colorado Avenue
Santa Monica, California
Phone: EX 39411

*LLOYD C. SCHUKNECHT, Jr.
Stanford Research Institute
Menlo Park, California
Phone: 326-6200, Ext. 3875

JOHN SHUNNY
Sandia Corporation
Sandia Base
Albuquerque, New Mexico
Phone: 264-3170

A. MACNEIL STELLE, Jr.
Atomics International
Los Angeles, California
Phone: DI 11000

WILLIAM R. STOBIE, Jr.
Lockheed Missiles and Space Company
111 Lockheed Way
Sunnyvale, California
Phone: RE 94321, Ext. 21735

WILLIAM SULLIVAN
Lockheed Missiles and Space Company
P.O. Box 504
Sunnyvale, California
Phone: 739-4321

*EUGENE J. SUTO
Research Analysis Corporation
McLean, Virginia
Phone: 893-5900, Ext. 581

EDWARD A. THOMPSON
 Lockheed Missiles and Space Company
 P.O. Box 504
 Sunnyvale, California
 Phone: RE 94321, Ext. 28316

**JAMES C. TROSINO
 Avco Corporation
 201 Lowell Street
 Wilmington, Massachusetts
 Phone: OL 88911, Ext. 2474

KENNETH R. UNLAND
 TRW Space Technology Laboratories
 Norton Air Force Base, California
 Phone: TUrner 94411, Ext. 8391

PHYLLIS A. VOGT
 Defense Atomic Support Agency
 Washington, D.C.
 Phone: OXford 54318

HAMPTON F. WLED
 Lockheed Missiles and Space Company
 P.O. Box 504
 Sunnyvale, California
 Phone: RE 94321, Ext. 21597

*ROBERT F. WHIPP
 United States Department of State
 Washington, D.C.
 Phone: DU 36428

H. RICHARD WILSON
 Lockheed Missiles and Space Company
 P.O. Box 504
 Sunnyvale, California
 Phone: RE 94321, Ext. 21556

RICHARD L. WILSON
 System Development Corporation
 2500 Colorado Avenue
 Santa Monica, California
 Phone: EX 39411

JOHN W. WISE
 Lockheed Missiles and Space Company
 P.O. Box 504
 Sunnyvale, California
 Phone: RE 94321, Ext. 22173, 20239

**DONALD B. WOODBRIDGE
 Union Carbide Nuclear Company
 Oak Ridge, Tennessee
 Phone:

W. DONALD ZIESEL
 Rohm & Haas Company
 222 West Washington Square
 Philadelphia, Pennsylvania
 Phone: WA 5-9860

*CHARTER MEMBERS OF RECORD ACTIVE

**CHARTER MEMBERS OF RECORD (LIFE MEMBERS—
 RETIRED)

FIRST NATIONAL SEMINAR

the National Classification Management Society Inc.

A NON-PROFIT ORGANIZATION

AN OPEN INVITATION TO THE FIRST NATIONAL SEMINAR
International Conference Room
Department of State
Washington, D.C.
July 13 - 14, 1965

Recognizing that security classification has become a highly specialized career field, a group of people from government and industry chartered the National Classification Management Society as a non-profit organization in 1964.

The principal objectives of the Society are to foster the development and exchange of information covering the following:

1. Systems and techniques for identifying information and material that require protection in the interests of national defense and security.
2. Procedures and practices for the management of classified material inventory.
3. Procedures and practices for identifying industrial, private or proprietary information as distinguished from classified information.
4. Methods for indoctrination and training of personnel in the application of accepted classification policies, procedures and requirements.

This Society will provide advice, assistance, ideas and techniques to make classification management an effective tool in enhancing the national security and defense of the United States. This will be accomplished in a professional manner without engaging in classified matters.

This new and growing organization will hold its First National Seminar on July 13-14, 1965, to provide a forum for public discussion of classification management. The seminar will be held in the International Conference Room, Diplomatic Entrance, 4000 Street Side, Department of State, Washington, D.C.

The registration fee of \$10.00 (\$15.00 for husband and wife) will cover the cost of publishing a report of the seminar and the NCMS President's Reception at Bolling Air Force Base Officer's Club on Tuesday Evening, July 13th.

Advance registration is required. Checks made out to the Society and the enclosed registration card should be sent to the Seminar Treasurer at the following address:

Mr. Eugene J. Suto
6116 Roseland Lane
Rockville, Maryland 20852

The public is cordially invited to attend all sessions of the seminar. Copies of the report of the seminar will be mailed to all paid registrants.

Yours truly,

Richard L. Durham
Richard L. Durham
Chairman
First National Seminar

Enclosures -

- (1) Seminar Program
- (2) Registration Card
- (3) Return Addressed Envelope

Chairman of the Board
DONALD G. GORRISON
United States National Bank
Washington, D.C.

PRESIDENT
ROBERT J. BUCKLAND
Lockheed Services Co.
Great Neck, N.Y.
Buckland & Co., Inc.

VICE PRESIDENT
RICHARD L. DURHAM
U.S. Navy Reserve
Baltimore, Md.
Department of State

SECRETARY TREASURER
EUGENE J. SUTO
The Great Falls Lodge, Inc.
Baltimore, Md.
Baltimore, Md.

Director
ROBERT G. MILLER
Baltimore, Md.
Baltimore, Md.

Director
RICHARD A. EDWARDS
The U.S. Navy
Baltimore, Md.
Baltimore, Md.

Director
DR. FRED L. BOWMAN
The U.S. Navy
Baltimore, Md.
Baltimore, Md.

ADVANCE RESERVATIONS - \$10.00 for
Conferees (\$15.00 for husband and wife)
- includes President's Reception

Send to: Mr. Eugene J. Suto
6116 Roseland Lane
Rockville, Maryland 20852

SOME PAST PRESIDENTS

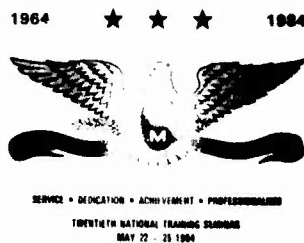


Left to Right—Al Thompson, Fred Daigle, Jim Mathena, Dean Richardson, Jim Buckland, Marilyn Griffin, Chris DeAngelis, Jim Bagley, Jack Robinson, Gene Suto

OPENING CEREMONIES 20th NATIONAL SEMINAR



Mike Lower, Seminar
Chairman



NCMS Seminar Logo



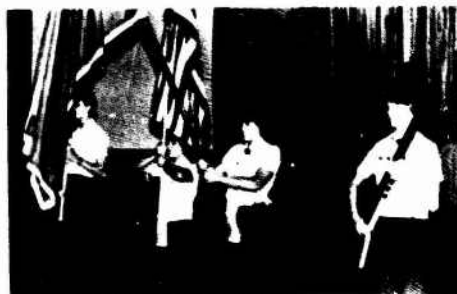
John Puckett, President
NCMS, reads President
Reagan's Greetings (see
Forward to Journal)



Fred Daigle with display of
founders & past presidents



Fred Daigle with display of
charter members



Honor Guard



NCMS National Officers



Seminar attendees



Country Store

AWARDS



Gene Suto
Woodbridge Award Winner



John Puckett,
President receives traditional gavel



Pam Hart, Vice President
Receives certificate of appreciation



Jerry Berkin, Director
Receives certificate of appreciation



Elaine Gruber, Director
Receives certificate of appreciation

**PRESIDENT JOHN PUCKETT PRESENTS
CERTIFICATES OF APPRECIATION**



Mike Lower, left, Seminar Chairman



Bill Johnson, right, Director



Liz Heinbuch, right, Director



**Ellen Herndon, right, chapter
chairperson, Florida Chapter**



**Michael Corbin, right, chapter
chairperson, Gulfcoast Chapter**



**Terris Lewis, right, chairperson, Mid-South
Chapter**



**Neil Self, right, Texas Gulfcoast
Chapter**

ANNIVERSARY PARTY



20th Anniversary Cake



ANNIVERSARY PARTY



CHARTER MEMBERS
Receive Special 20th Anniversary paper
weights from President John Puckett



Fred Daigle



Gene Suto



Jim Bagley



Fred Koether



Francis Jahn



Tony Correia



Lorry McConnell



Jim Trosino



Lloyd Schuknecht

SEMINAR SPEAKERS



Maynard C. Anderson



Thomas C. O'Brien



Allan E. Suchinsky



Joseph J. Tate



Thomas J. Conner



Irving T. Boker



James Mood



Anthony G. Mitchell



David Whitman



James Bagley



James Dearlove



John McMichael



Robert Grogan



David C. Brown



Robert Fredlund



Joseph Cacek



Gerald Berken



Joseph Murray



Frederick Daigle

WORKSHOP SPEAKERS
Seminar Committee & Board of Directors



Andrea Wraalstad, DIS



Maria Barela, DOE



Joe Grau, DSI



Ron Weaver, Navy



Graham King, AFSC



Dave Whitman, DOD



Sheila Daigle, DIS



George Carnahan, DOE



Herman Teifeld, LLNL



Seminar Committee



Current Board of Directors



President Elect, Pam Hart, with Husband's Bouquet!



President & Mrs. John Puckett